Exhibit P

EXHIBIT D-1
Invalidity of U.S. Patent No. 9,215,613 in view of U.S. Patent Pub. No. 2008/0160958 ("Abichandani")

U.S. Patent Publication No. 2008/0160958 ("Abichandani") was published on July 3, 2008 and therefore constitutes prior art under at least 35 U.S.C. §§ 102(a), (b), and/or (e) as to the Asserted Claims of U.S. Pat. No. 9,215,613 ("the '613 Patent"). Abichandani anticipates and/or renders obvious the Asserted Claims, either alone or in combination with one or more references identified in Defendants' Cover Pleading.

To the extent Plaintiff argues that Abichandani does not disclose any element below, a person of ordinary skill in the art would have found it obvious in view of Abichandani alone, with the knowledge of a person of ordinary skill in the art, and/or in view of the prior art systems and references disclosed in § II of Defendants' Invalidity Contentions and the exemplary citations and commentary provided for this claim in Exhibits D-2 to D-17 and Appendix D-D thereto. A person of ordinary skill in the art would have been motivated to combine and would have a reasonable expectation of success in combining these references because the cited references relate to the same technical field as Abichandani (i.e., network and device management).

The chart below provides representative examples of where each element is found within Abichandani. Citations are meant to be exemplary, not exhaustive, and Defendants reserve the right to identify and discuss additional portions of the reference in support of its contentions and/or to rebut arguments made by Plaintiff. Citations to figures, drawings, tables, and the like include reference to any accompanying or related text. All internal cross references are meant to incorporate the cross-referenced material as if fully set forth therein.

It is Defendants' position that Plaintiff's Disclosure of Asserted Claims and Infringement Contentions have not established that any accused product or service infringes any valid claim. Thus, Defendants' statements below should not be treated as an admission, implication, or suggestion that Defendants agree with Plaintiff regarding either the scope, construction, or interpretation of any of the Asserted Claims of the infringement theories advanced by Plaintiff in its Preliminary Infringement Contentions, including whether any Asserted Claims satisfies 35 U.S.C. §§ 101 or 112. In certain cases, Defendants specify non-limiting examples of where its application of the prior art is based on Plaintiff's apparent application of the claim element. These statements are not intended to suggest that Defendants agree with Plaintiff's application of any claim term, suggest a proposed construction at this stage of the case, or suggest that construction is needed, as the parties are not required to exchange terms for construction or proposed constructions until a later date.

Plaintiff has yet to identify of the Asserted Claims that it contends is not anticipated and/or rendered obvious by Abichandani. Defendants therefore expressly reserve the right to respond to any such contention, including by identifying additional obviousness combinations, if Plaintiff makes any such contention.

Where Defendants state that Abichandani "discloses" a limitation, that disclosure may be express, implicit, and/or inherent.

U.S. Patent No. US 9,215,613 (the "'613 Patent")	
Claim Language	**Exemplary Disclosure of Abichandani**
1. A wireless end-user device, comprising:	To the extent the preamble may be limiting, Abichandani discloses the preamble. For example: **[Abstract]** A system and method are described whereby a mobile device controls access to mobile applications based on access conditions associated with a current access network. To prevent mobile applications from running when the access conditions are not suitable, the mobile device includes a policy database used to store a list of access conditions that are inappropriate for launching the installed applications. The access conditions are based on the type of the current access network used by the mobile device for launching or maintaining the requested application session. The access conditions indicate whether the mobile device is currently accessing its home network or roaming on another provider's network. Similarly, the access conditions indicate the type of network access interface used by the current network to provide the data connection necessary to run the requested application. The policy database correlates predetermined actions with the access conditions associated with a given application session. **[0004]** Embodiments of the invention are used to provide a system and method for controlling access to mobile applications from the mobile device based on access conditions associated with a current access network, To prevent one or more applications or services from running when the access conditions are not suitable, the memory of the mobile device includes a policy or application access database, which is used to store a list of access conditions that are inappropriate for launching the installed applications. In embodiments, the access conditions are based on the type of the current access network used by the mobile device for launching or maintaining the requested application session. For example, the access conditions may indicate whether the mobile device is currently accessing its home network or roaming on another provider's network. Similarly, the access conditions may indicate the type of network access interface used by the current network to provide the data connection necessary to run the requested application. The policy database correlates predetermined actions with current status of access conditions associated with a given application session. In one embodiment, when the mobile device accesses a network having an access technology specification with insufficient data handling capabilities for the requested application, the mobile device denies access to the data-intensive application or service specified in the policy database. Similarly, to avoid unwanted roaming charges, the mobile device's policy database includes instructions to suspend any scheduled firmware updates via a firmware over the air (FOTA) application until the mobile device returns to its home network. **[0005]** In one aspect of the invention, a method is provided for controlling access to an application, the application capable of running on a mobile device by connecting to an access network, the method comprising registering the application with the mobile device, populating a record on the mobile device, the record specifying one or more conditions for controlling access to the application, the one or more conditions

	associated with the access network, monitoring the one or more conditions, and controlling access to the application from the mobile device based on the one or more conditions. **[0006]** In another aspect of the invention, a mobile device is provided, the mobile device capable of running an application by connecting to an access network, the mobile device comprising a processor, a wireless interface for connecting to the access network, and a computer readable medium having thereon instructions for registering the application with the mobile device, populating a record on the mobile device, the record specifying one or more conditions for controlling access to the application, the one or more conditions associated with the access network, monitoring the one or more conditions, and controlling access to the application from the mobile device based on the one or more conditions. **[0007]** In still another aspect of the invention, a system is provided for controlling access to an application, the application capable of running on a mobile device by connecting to an access network, the system comprising (a) the mobile device capable of storing a record for specifying one or more conditions for controlling access to the application, the one or more conditions associated with the access network, the mobile device comprising an access network monitor module configured to monitor the one or more conditions, and an application manager module configured to control access to the application from the mobile device based on the one or more conditions reported by the access network monitor module, and (b) a device management server having a management connection to the mobile device for populating the record. To the extent Abichandani does not explicitly and/or inherently disclose this element, it would have been obvious in view of the knowledge of a person of ordinary skill in the art in light of Abichandani alone or it would have been obvious to combine Abichandani with one or more prior art references charted in these Invalidity Contentions or identified in the cover document to which this chart is attached.
(a) a wireless wide area network (WWAN) modem to communicate data for Internet service activities between the device and at least one WWAN, when configured for and connected to the WWAN;	Abichandani discloses this limitation. For example: **[Abstract]** A system and method are described whereby a mobile device controls access to mobile applications based on access conditions associated with a current access network. To prevent mobile applications from running when the access conditions are not suitable, the mobile device includes a policy database used to store a list of access conditions that are inappropriate for launching the installed applications. The access conditions are based on the type of the current access network used by the mobile device for launching or maintaining the requested application session. The access conditions indicate whether the mobile device is currently accessing its home network or roaming on another provider's network. Similarly, the access conditions indicate the type of network access interface used by the current network to provide the data connection necessary to run the requested application. The policy database correlates predetermined actions with the access conditions associated with a given application session.

	[0004] Embodiments of the invention are used to provide a system and method for controlling access to mobile applications from the mobile device based on access conditions associated with a current access network, To prevent one or more applications or services from running when the access conditions are not suitable, the memory of the mobile device includes a policy or application access database, which is used to store a list of access conditions that are inappropriate for launching the installed applications. In embodiments, the access conditions are based on the type of the current access network used by the mobile device for launching or maintaining the requested application session. For example, the access conditions may indicate whether the mobile device is currently accessing its home network or roaming on another provider's network. Similarly, the access conditions may indicate the type of network access interface used by the current network to provide the data connection necessary to run the requested application. The policy database correlates predetermined actions with current status of access conditions associated with a given application session. In one embodiment, when the mobile device accesses a network having an access technology specification with insufficient data handling capabilities for the requested application, the mobile device denies access to the data-intensive application or service specified in the policy database. Similarly, to avoid unwanted roaming charges, the mobile device's policy database includes instructions to suspend any scheduled firmware updates via a firmware over the air (FOTA) application until the mobile device returns to its home network. **[0005]** In one aspect of the invention, a method is provided for controlling access to an application, the application capable of running on a mobile device by connecting to an access network, the method comprising registering the application with the mobile device, populating a record on the mobile device, the record specifying one or more conditions for controlling access to the application, the one or more conditions associated with the access network, monitoring the one or more conditions, and controlling access to the application from the mobile device based on the one or more conditions. **[0006]** In another aspect of the invention, a mobile device is provided, the mobile device capable of running an application by connecting to an access network, the mobile device comprising a processor, a wireless interface for connecting to the access network, and a computer readable medium having thereon instructions for registering the application with the mobile device, populating a record on the mobile device, the record specifying one or more conditions for controlling access to the application, the one or more conditions associated with the access network, monitoring the one or more conditions, and controlling access to the application from the mobile device based on the one or more conditions. **[0007]** In still another aspect of the invention, a system is provided for controlling access to an application, the application capable of running on a mobile device by connecting to an access network, the system comprising (a) the mobile device capable of storing a record for specifying one or more conditions for controlling access

	to the application, the one or more conditions associated with the access network, the mobile device comprising an access network monitor module configured to monitor the one or more conditions, and an application manager module configured to control access to the application from the mobile device based on the one or more conditions reported by the access network monitor module, and (b) a device management server having a management connection to the mobile device for populating the record. **[0013]** Turning to FIG. 1, an implementation of a system contemplated by an embodiment of the invention is shown with reference to a mobile network environment. In the illustrated embodiment, the user device 100 is a mobile device, such as a wireless telephone or a portable computer capable of launching an application by connecting to an application server 106 via one or more access networks 102, 104. The application server 106 is responsible for content delivery to the one or more applications running on a mobile device 100. For example, when the mobile device 100 includes a multimedia streaming application, the application server 106 employs a Real-Time Transfer Protocol (RTP) to stream the requested content to the multimedia streaming application launched on the mobile device 100. In this embodiment, the application server 106 is part of a core network 108, which is an IP Multimedia Services (IMS) network responsible for session control and Quality of Service (QoS) management of ongoing application sessions. Alternately, the application server 106 is located outside of the core network 108, whereby the core network 108 connects to the application server 106 via the Internet 110. In embodiments where the IMS core network 108 is not implemented, the application server 106 may be part of one of the access networks 102, 104, for example, or it may connect to the access networks 102, 104 via the Internet 110. **[0014]** As illustrated in FIG. 1, the access networks 102, 104 interface with the mobile device 100 in accordance with a network interface specification 112. Preferably, the network interface specification 112 complies with one or more wireless access standards, each having corresponding data handling capabilities, such as average and maximum uplink/downlink throughput speeds. In embodiments, the wireless network standards include CDMA 2000 1X, 1xEV-DO, 1xEV-DV, EDGE, and HSPDA network technologies, or combinations thereof In order to launch the application 106, the mobile device 100 typically accesses its home network 102. However, when the access network 102 is not available, such as when the mobile device 100 travels outside of its home coverage area, the mobile device 100 is capable of launching the application 106 via a roaming network 104. **[0015]** Turning to FIG. 2, embodiments of the mobile device 200 and networks 214, 220 are provided in accordance with an embodiment of the present invention, wherein the mobile device 200 controls access to one or more applications 202-206 based on access conditions associated with the access networks 214, 220. The mobile device 200 is capable of launching one or more applications 202-206 from its memory. The applications 202-206 include multimedia, voice, email, instant messaging, text messaging, firmware update, or any other applications or services requiring access to the home network 214 or roaming network 220 to

	establish an application session. In the illustrated embodiment, the memory of the mobile device 200 includes a Firmware Update Over the Air (FOTA) application 202, a Voice over IP (VoIP) application 204, and a video streaming application 206. **[0016]** To prevent one or more applications or services 202-206 from running when the access conditions are not suitable, the memory of the mobile device 200 includes a policy or application access database 212, which is used to store a list of access conditions that are inappropriate for launching the applications 202-206. Specifically, the access conditions are based on the type of the current access network used by the mobile device 200 for launching or maintaining the requested application session 202-206. For example, the access conditions may indicate whether the mobile device is currently accessing its home network 214 or roaming on the network 220. Similarly, the access conditions may indicate the type of network access interface or standard used by the current network 214, 220 to provide data connection necessary to run the application 202-206. The following table illustrates an example of the policy database 212 having a list of applications and corresponding access conditions, which in this embodiment are designated as inappropriate for allowing access to the listed applications or services. **[0017]** Alternatively, the database 212 may contain a list of application/access condition pairs under which access to the requested applications or services is allowed. In embodiments, the policy database 212 includes application types, such as "video streaming" and/or associated application names, such as "Windows Media Player," for example. As illustrated above, the policy database 212 correlates predetermined actions with current status of access conditions associated with a given application session. When the mobile device 200 registers with an access network having a network access technology specification 222 with insufficient data handling capabilities for the requested application, the mobile device 200 is instructed to deny access to a data-intensive application or service specified in the database or lookup table 212. For example, the mobile device 200 is instructed to deny access to a video streaming or VoIP application session when the access conditions indicate that the mobile device 200 is currently using a CDMA 2000 1x network access technology. This avoids unnecessary use of network resources which, under current access conditions, are incapable of providing a satisfying user experience for the desired application. On the other hand, if the current access conditions do not match those in the policy database 212, such as when the mobile device 200 is registered with an EVDO access network, a user is granted full access to the desired video streaming or VoIP applications. Similarly, to avoid unwanted roaming charges, the policy database 212 includes instructions to suspend any scheduled firmware updates via a FOTA application until the mobile device 200 returns to the home network 214. **[0018]** Preferably, the policy database 212 is populated by a network provider using conventional Over the Air Device Management (OTA DM) technology to provide the network operator with full control over the

	contents of the database 212. In an embodiment, the policy database 212 is centrally populated, distributed, and updated over the air for each mobile device 200 via a management console 218 connected to a device management server 216. The network provider may choose to distribute the policy database 212 according to different classes of mobile devices 200, wherein each device class designates the types of access networks accessible to the device 200, as well as the types of applications installed in its memory. The management console 218, as well as the device management server 216, are located within the home access network 214 or may be collocated with the network administration equipment at a network operations center (NOC) or at a mobile switching center (MSC), for example. **[0019]** As further illustrated in FIG. 2, to gain access to the network resources, the application 202-206 registers with an application manager 210. Specifically, when a user attempts to launch an application 202-206, the application 202-206 supplies its name and/or type information to the application manager 210, which, in turn, receives an input of the monitored access conditions from the access network monitor 208. The application manager 210 queries the policy database 212 for the corresponding application/access condition entry and denies access to the application if a match is found. Otherwise, the mobile device 200 initiates the application session over the current access network 214, 220. In a further embodiment, the access network monitor 208 continues to report the changes in current access conditions during the application session to allow the application manager 210 to terminate the application when a change in the access conditions matches an entry in the policy database 212. **[0020]** In this embodiment, the application manager 210 and the access network monitor 208 are implemented as Binary Runtime Environment for Wireless (BREW) software modules exposing standard interfaces for interaction with other software components of the mobile device 200 via an application programming interface (API). Other embodiments of the application manager 210 and access network monitor 208 include using a Java-based implementation capable of running on a plurality of mobile phone operating systems, such as Symbian, Windows Mobile Edition, or Palm, for example. **[0021]** Turning to FIG. 3, an embodiment of a method for controlling access to applications from a mobile device 200 is illustrated with reference to an exemplary message flow scenario. In step 300, the device management server 216 updates the policy database 212 when new applications or services are introduced by the network operator or pursuant to setting up a new customer account. In step 302, when the user requests to launch a video streaming application 206, the application 206 registers with the application manager 210 by providing it with its name and/or type information, such as “Windows Media Player”/“video streaming,” for example. This prompts the application manager 2 10 to request and receive the current access condition information from the access network monitor 208, steps 304-306. In this embodiment, the access condition information includes information regarding the current access network, such as roaming status and compatible

	network access technology. In steps 308-310, based on the received application information, the application manager 210 requests and receives one or more entries from the policy database 212 indicating which access conditions preclude the establishment of an application session for the application 206. In step 312, the application manager allows the user to launch the requested application if the current access conditions do not match any of the entries returned by the policy database 212 that require denial or suspension of access to the application. In this embodiment, upon establishment of the application session, the access network monitor 208 continuously monitors any changes in the current access conditions. Therefore, when, in step 314, the access network monitor 208 detects a change in the access conditions, for example when the mobile device 200 migrates from an EVDO to a CDMA 2000 1X access network overlay, it notifies the application manager 210 accordingly. Since this change in the access conditions matches an entry received from the policy database 212 requiring denial of access to the application, the application manager 210, in step 316, sends an event to the application 206 ending the current application session by forcing it to quit. *See* Figs. 1, 2 & 3. To the extent Abichandani does not explicitly and/or inherently disclose this element, it would have been obvious in view of the knowledge of a person of ordinary skill in the art in light of Abichandani alone or it would have been obvious to combine Abichandani with one or more prior art references charted in these Invalidity Contentions or identified in the cover document to which this chart is attached.
(b) a wireless local area network (WLAN) modem to communicate data for Internet service activities between the device and at least one WLAN, when configured for and connected to the WLAN;	Abichandani discloses this limitation. For example: **[Abstract]** A system and method are described whereby a mobile device controls access to mobile applications based on access conditions associated with a current access network. To prevent mobile applications from running when the access conditions are not suitable, the mobile device includes a policy database used to store a list of access conditions that are inappropriate for launching the installed applications. The access conditions are based on the type of the current access network used by the mobile device for launching or maintaining the requested application session. The access conditions indicate whether the mobile device is currently accessing its home network or roaming on another provider's network. Similarly, the access conditions indicate the type of network access interface used by the current network to provide the data connection necessary to run the requested application. The policy database correlates predetermined actions with the access conditions associated with a given application session. **[0004]** Embodiments of the invention are used to provide a system and method for controlling access to mobile applications from the mobile device based on access conditions associated with a current access network, To prevent one or more applications or services from running when the access conditions are not suitable, the memory of the mobile device includes a policy or application access database, which is used to

	store a list of access conditions that are inappropriate for launching the installed applications. In embodiments, the access conditions are based on the type of the current access network used by the mobile device for launching or maintaining the requested application session. For example, the access conditions may indicate whether the mobile device is currently accessing its home network or roaming on another provider's network. Similarly, the access conditions may indicate the type of network access interface used by the current network to provide the data connection necessary to run the requested application. The policy database correlates predetermined actions with current status of access conditions associated with a given application session. In one embodiment, when the mobile device accesses a network having an access technology specification with insufficient data handling capabilities for the requested application, the mobile device denies access to the data-intensive application or service specified in the policy database. Similarly, to avoid unwanted roaming charges, the mobile device's policy database includes instructions to suspend any scheduled firmware updates via a firmware over the air (FOTA) application until the mobile device returns to its home network. **[0005]** In one aspect of the invention, a method is provided for controlling access to an application, the application capable of running on a mobile device by connecting to an access network, the method comprising registering the application with the mobile device, populating a record on the mobile device, the record specifying one or more conditions for controlling access to the application, the one or more conditions associated with the access network, monitoring the one or more conditions, and controlling access to the application from the mobile device based on the one or more conditions. **[0006]** In another aspect of the invention, a mobile device is provided, the mobile device capable of running an application by connecting to an access network, the mobile device comprising a processor, a wireless interface for connecting to the access network, and a computer readable medium having thereon instructions for registering the application with the mobile device, populating a record on the mobile device, the record specifying one or more conditions for controlling access to the application, the one or more conditions associated with the access network, monitoring the one or more conditions, and controlling access to the application from the mobile device based on the one or more conditions. **[0007]** In still another aspect of the invention, a system is provided for controlling access to an application, the application capable of running on a mobile device by connecting to an access network, the system comprising (a) the mobile device capable of storing a record for specifying one or more conditions for controlling access to the application, the one or more conditions associated with the access network, the mobile device comprising an access network monitor module configured to monitor the one or more conditions, and an application manager module configured to control access to the application from the mobile device based on the one or more conditions reported by the access network monitor module, and (b) a device management server having a management connection to the mobile device for populating the record.

	[0013] Turning to FIG. 1, an implementation of a system contemplated by an embodiment of the invention is shown with reference to a mobile network environment. In the illustrated embodiment, the user device 100 is a mobile device, such as a wireless telephone or a portable computer capable of launching an application by connecting to an application server 106 via one or more access networks 102, 104. The application server 106 is responsible for content delivery to the one or more applications running on a mobile device 100. For example, when the mobile device 100 includes a multimedia streaming application, the application server 106 employs a Real-Time Transfer Protocol (RTP) to stream the requested content to the multimedia streaming application launched on the mobile device 100. In this embodiment, the application server 106 is part of a core network 108, which is an IP Multimedia Services (IMS) network responsible for session control and Quality of Service (QoS) management of ongoing application sessions. Alternately, the application server 106 is located outside of the core network 108, whereby the core network 108 connects to the application server 106 via the Internet 110. In embodiments where the IMS core network 108 is not implemented, the application server 106 may be part of one of the access networks 102, 104, for example, or it may connect to the access networks 102, 104 via the Internet 110. **[0014]** As illustrated in FIG. 1, the access networks 102, 104 interface with the mobile device 100 in accordance with a network interface specification 112. Preferably, the network interface specification 112 complies with one or more wireless access standards, each having corresponding data handling capabilities, such as average and maximum uplink/downlink throughput speeds. In embodiments, the wireless network standards include CDMA 2000 1X, 1xEV-DO, 1xEV-DV, EDGE, and HSPDA network technologies, or combinations thereof In order to launch the application 106, the mobile device 100 typically accesses its home network 102. However, when the access network 102 is not available, such as when the mobile device 100 travels outside of its home coverage area, the mobile device 100 is capable of launching the application 106 via a roaming network 104. **[0015]** Turning to FIG. 2, embodiments of the mobile device 200 and networks 214, 220 are provided in accordance with an embodiment of the present invention, wherein the mobile device 200 controls access to one or more applications 202-206 based on access conditions associated with the access networks 214, 220. The mobile device 200 is capable of launching one or more applications 202-206 from its memory. The applications 202-206 include multimedia, voice, email, instant messaging, text messaging, firmware update, or any other applications or services requiring access to the home network 214 or roaming network 220 to establish an application session. In the illustrated embodiment, the memory of the mobile device 200 includes a Firmware Update Over the Air (FOTA) application 202, a Voice over IP (VoIP) application 204, and a video streaming application 206.

	[0016] To prevent one or more applications or services 202-206 from running when the access conditions are not suitable, the memory of the mobile device 200 includes a policy or application access database 212, which is used to store a list of access conditions that are inappropriate for launching the applications 202-206. Specifically, the access conditions are based on the type of the current access network used by the mobile device 200 for launching or maintaining the requested application session 202-206. For example, the access conditions may indicate whether the mobile device is currently accessing its home network 214 or roaming on the network 220. Similarly, the access conditions may indicate the type of network access interface or standard used by the current network 214, 220 to provide data connection necessary to run the application 202-206. The following table illustrates an example of the policy database 212 having a list of applications and corresponding access conditions, which in this embodiment are designated as inappropriate for allowing access to the listed applications or services. **[0017]** Alternatively, the database 212 may contain a list of application/access condition pairs under which access to the requested applications or services is allowed. In embodiments, the policy database 212 includes application types, such as "video streaming" and/or associated application names, such as "Windows Media Player," for example. As illustrated above, the policy database 212 correlates predetermined actions with current status of access conditions associated with a given application session. When the mobile device 200 registers with an access network having a network access technology specification 222 with insufficient data handling capabilities for the requested application, the mobile device 200 is instructed to deny access to a data-intensive application or service specified in the database or lookup table 212. For example, the mobile device 200 is instructed to deny access to a video streaming or VoIP application session when the access conditions indicate that the mobile device 200 is currently using a CDMA 2000 1x network access technology. This avoids unnecessary use of network resources which, under current access conditions, are incapable of providing a satisfying user experience for the desired application. On the other hand, if the current access conditions do not match those in the policy database 212, such as when the mobile device 200 is registered with an EVDO access network, a user is granted full access to the desired video streaming or VoIP applications. Similarly, to avoid unwanted roaming charges, the policy database 212 includes instructions to suspend any scheduled firmware updates via a FOTA application until the mobile device 200 returns to the home network 214. **[0018]** Preferably, the policy database 212 is populated by a network provider using conventional Over the Air Device Management (OTA DM) technology to provide the network operator with full control over the contents of the database 212. In an embodiment, the policy database 212 is centrally populated, distributed, and updated over the air for each mobile device 200 via a management console 218 connected to a device management server 216. The network provider may choose to distribute the policy database 212 according to different classes of mobile devices 200, wherein each device class designates the types of access networks

	accessible to the device 200, as well as the types of applications installed in its memory. The management console 218, as well as the device management server 216, are located within the home access network 214 or may be collocated with the network administration equipment at a network operations center (NOC) or at a mobile switching center (MSC), for example. **[0019]** As further illustrated in FIG. 2, to gain access to the network resources, the application 202-206 registers with an application manager 210. Specifically, when a user attempts to launch an application 202-206, the application 202-206 supplies its name and/or type information to the application manager 210, which, in turn, receives an input of the monitored access conditions from the access network monitor 208. The application manager 210 queries the policy database 212 for the corresponding application/access condition entry and denies access to the application if a match is found. Otherwise, the mobile device 200 initiates the application session over the current access network 214, 220. In a further embodiment, the access network monitor 208 continues to report the changes in current access conditions during the application session to allow the application manager 210 to terminate the application when a change in the access conditions matches an entry in the policy database 212. **[0020]** In this embodiment, the application manager 210 and the access network monitor 208 are implemented as Binary Runtime Environment for Wireless (BREW) software modules exposing standard interfaces for interaction with other software components of the mobile device 200 via an application programming interface (API). Other embodiments of the application manager 210 and access network monitor 208 include using a Java-based implementation capable of running on a plurality of mobile phone operating systems, such as Symbian, Windows Mobile Edition, or Palm, for example. **[0021]** Turning to FIG. 3, an embodiment of a method for controlling access to applications from a mobile device 200 is illustrated with reference to an exemplary message flow scenario. In step 300, the device management server 216 updates the policy database 212 when new applications or services are introduced by the network operator or pursuant to setting up a new customer account. In step 302, when the user requests to launch a video streaming application 206, the application 206 registers with the application manager 210 by providing it with its name and/or type information, such as “Windows Media Player”/“video streaming,” for example. This prompts the application manager 2 10 to request and receive the current access condition information from the access network monitor 208, steps 304-306. In this embodiment, the access condition information includes information regarding the current access network, such as roaming status and compatible network access technology. In steps 308-310, based on the received application information, the application manager 210 requests and receives one or more entries from the policy database 212 indicating which access conditions preclude the establishment of an application session for the application 206. In step 312, the application manager allows the user to launch the requested application if the current access conditions do not

	match any of the entries returned by the policy database 212 that require denial or suspension of access to the application. In this embodiment, upon establishment of the application session, the access network monitor 208 continuously monitors any changes in the current access conditions. Therefore, when, in step 314, the access network monitor 208 detects a change in the access conditions, for example when the mobile device 200 migrates from an EVDO to a CDMA 2000 1X access network overlay, it notifies the application manager 210 accordingly. Since this change in the access conditions matches an entry received from the policy database 212 requiring denial of access to the application, the application manager 210, in step 316, sends an event to the application 206 ending the current application session by forcing it to quit. *See* Figs. 1, 2 & 3. To the extent Abichandani does not explicitly and/or inherently disclose this element, it would have been obvious in view of the knowledge of a person of ordinary skill in the art in light of Abichandani alone or it would have been obvious to combine Abichandani with one or more prior art references charted in these Invalidity Contentions or identified in the cover document to which this chart is attached.
(c) a non-transient memory to store	Abichandani discloses this limitation. For example: **[Abstract]** A system and method are described whereby a mobile device controls access to mobile applications based on access conditions associated with a current access network. To prevent mobile applications from running when the access conditions are not suitable, the mobile device includes a policy database used to store a list of access conditions that are inappropriate for launching the installed applications. The access conditions are based on the type of the current access network used by the mobile device for launching or maintaining the requested application session. The access conditions indicate whether the mobile device is currently accessing its home network or roaming on another provider's network. Similarly, the access conditions indicate the type of network access interface used by the current network to provide the data connection necessary to run the requested application. The policy database correlates predetermined actions with the access conditions associated with a given application session. **[0004]** Embodiments of the invention are used to provide a system and method for controlling access to mobile applications from the mobile device based on access conditions associated with a current access network, To prevent one or more applications or services from running when the access conditions are not suitable, the memory of the mobile device includes a policy or application access database, which is used to store a list of access conditions that are inappropriate for launching the installed applications. In embodiments, the access conditions are based on the type of the current access network used by the mobile device for launching or maintaining the requested application session. For example, the access conditions may indicate whether the mobile device is currently accessing its home network or roaming on another provider's network.

	Similarly, the access conditions may indicate the type of network access interface used by the current network to provide the data connection necessary to run the requested application. The policy database correlates predetermined actions with current status of access conditions associated with a given application session. In one embodiment, when the mobile device accesses a network having an access technology specification with insufficient data handling capabilities for the requested application, the mobile device denies access to the data-intensive application or service specified in the policy database. Similarly, to avoid unwanted roaming charges, the mobile device's policy database includes instructions to suspend any scheduled firmware updates via a firmware over the air (FOTA) application until the mobile device returns to its home network. **[0005]** In one aspect of the invention, a method is provided for controlling access to an application, the application capable of running on a mobile device by connecting to an access network, the method comprising registering the application with the mobile device, populating a record on the mobile device, the record specifying one or more conditions for controlling access to the application, the one or more conditions associated with the access network, monitoring the one or more conditions, and controlling access to the application from the mobile device based on the one or more conditions. **[0006]** In another aspect of the invention, a mobile device is provided, the mobile device capable of running an application by connecting to an access network, the mobile device comprising a processor, a wireless interface for connecting to the access network, and a computer readable medium having thereon instructions for registering the application with the mobile device, populating a record on the mobile device, the record specifying one or more conditions for controlling access to the application, the one or more conditions associated with the access network, monitoring the one or more conditions, and controlling access to the application from the mobile device based on the one or more conditions. **[0007]** In still another aspect of the invention, a system is provided for controlling access to an application, the application capable of running on a mobile device by connecting to an access network, the system comprising (a) the mobile device capable of storing a record for specifying one or more conditions for controlling access to the application, the one or more conditions associated with the access network, the mobile device comprising an access network monitor module configured to monitor the one or more conditions, and an application manager module configured to control access to the application from the mobile device based on the one or more conditions reported by the access network monitor module, and (b) a device management server having a management connection to the mobile device for populating the record. **[0013]** Turning to FIG. 1, an implementation of a system contemplated by an embodiment of the invention is shown with reference to a mobile network environment. In the illustrated embodiment, the user device 100 is a mobile device, such as a wireless telephone or a portable computer capable of launching an application by

	connecting to an application server 106 via one or more access networks 102, 104. The application server 106 is responsible for content delivery to the one or more applications running on a mobile device 100. For example, when the mobile device 100 includes a multimedia streaming application, the application server 106 employs a Real-Time Transfer Protocol (RTP) to stream the requested content to the multimedia streaming application launched on the mobile device 100. In this embodiment, the application server 106 is part of a core network 108, which is an IP Multimedia Services (IMS) network responsible for session control and Quality of Service (QoS) management of ongoing application sessions. Alternately, the application server 106 is located outside of the core network 108, whereby the core network 108 connects to the application server 106 via the Internet 110. In embodiments where the IMS core network 108 is not implemented, the application server 106 may be part of one of the access networks 102, 104, for example, or it may connect to the access networks 102, 104 via the Internet 110. **[0014]** As illustrated in FIG. 1, the access networks 102, 104 interface with the mobile device 100 in accordance with a network interface specification 112. Preferably, the network interface specification 112 complies with one or more wireless access standards, each having corresponding data handling capabilities, such as average and maximum uplink/downlink throughput speeds. In embodiments, the wireless network standards include CDMA 2000 1X, 1xEV-DO, 1xEV-DV, EDGE, and HSPDA network technologies, or combinations thereof In order to launch the application 106, the mobile device 100 typically accesses its home network 102. However, when the access network 102 is not available, such as when the mobile device 100 travels outside of its home coverage area, the mobile device 100 is capable of launching the application 106 via a roaming network 104. **[0015]** Turning to FIG. 2, embodiments of the mobile device 200 and networks 214, 220 are provided in accordance with an embodiment of the present invention, wherein the mobile device 200 controls access to one or more applications 202-206 based on access conditions associated with the access networks 214, 220. The mobile device 200 is capable of launching one or more applications 202-206 from its memory. The applications 202-206 include multimedia, voice, email, instant messaging, text messaging, firmware update, or any other applications or services requiring access to the home network 214 or roaming network 220 to establish an application session. In the illustrated embodiment, the memory of the mobile device 200 includes a Firmware Update Over the Air (FOTA) application 202, a Voice over IP (VoIP) application 204, and a video streaming application 206. **[0016]** To prevent one or more applications or services 202-206 from running when the access conditions are not suitable, the memory of the mobile device 200 includes a policy or application access database 212, which is used to store a list of access conditions that are inappropriate for launching the applications 202-206. Specifically, the access conditions are based on the type of the current access network used by the mobile device 200 for launching or maintaining the requested application session 202-206. For example, the access

	conditions may indicate whether the mobile device is currently accessing its home network 214 or roaming on the network 220. Similarly, the access conditions may indicate the type of network access interface or standard used by the current network 214, 220 to provide data connection necessary to run the application 202-206. The following table illustrates an example of the policy database 212 having a list of applications and corresponding access conditions, which in this embodiment are designated as inappropriate for allowing access to the listed applications or services. **[0017]** Alternatively, the database 212 may contain a list of application/access condition pairs under which access to the requested applications or services is allowed. In embodiments, the policy database 212 includes application types, such as "video streaming" and/or associated application names, such as "Windows Media Player," for example. As illustrated above, the policy database 212 correlates predetermined actions with current status of access conditions associated with a given application session. When the mobile device 200 registers with an access network having a network access technology specification 222 with insufficient data handling capabilities for the requested application, the mobile device 200 is instructed to deny access to a data-intensive application or service specified in the database or lookup table 212. For example, the mobile device 200 is instructed to deny access to a video streaming or VoIP application session when the access conditions indicate that the mobile device 200 is currently using a CDMA 2000 1x network access technology. This avoids unnecessary use of network resources which, under current access conditions, are incapable of providing a satisfying user experience for the desired application. On the other hand, if the current access conditions do not match those in the policy database 212, such as when the mobile device 200 is registered with an EVDO access network, a user is granted full access to the desired video streaming or VoIP applications. Similarly, to avoid unwanted roaming charges, the policy database 212 includes instructions to suspend any scheduled firmware updates via a FOTA application until the mobile device 200 returns to the home network 214. **[0018]** Preferably, the policy database 212 is populated by a network provider using conventional Over the Air Device Management (OTA DM) technology to provide the network operator with full control over the contents of the database 212. In an embodiment, the policy database 212 is centrally populated, distributed, and updated over the air for each mobile device 200 via a management console 218 connected to a device management server 216. The network provider may choose to distribute the policy database 212 according to different classes of mobile devices 200, wherein each device class designates the types of access networks accessible to the device 200, as well as the types of applications installed in its memory. The management console 218, as well as the device management server 216, are located within the home access network 214 or may be collocated with the network administration equipment at a network operations center (NOC) or at a mobile switching center (MSC), for example.

	[0019] As further illustrated in FIG. 2, to gain access to the network resources, the application 202-206 registers with an application manager 210. Specifically, when a user attempts to launch an application 202-206, the application 202-206 supplies its name and/or type information to the application manager 210, which, in turn, receives an input of the monitored access conditions from the access network monitor 208. The application manager 210 queries the policy database 212 for the corresponding application/access condition entry and denies access to the application if a match is found. Otherwise, the mobile device 200 initiates the application session over the current access network 214, 220. In a further embodiment, the access network monitor 208 continues to report the changes in current access conditions during the application session to allow the application manager 210 to terminate the application when a change in the access conditions matches an entry in the policy database 212. **[0020]** In this embodiment, the application manager 210 and the access network monitor 208 are implemented as Binary Runtime Environment for Wireless (BREW) software modules exposing standard interfaces for interaction with other software components of the mobile device 200 via an application programming interface (API). Other embodiments of the application manager 210 and access network monitor 208 include using a Java-based implementation capable of running on a plurality of mobile phone operating systems, such as Symbian, Windows Mobile Edition, or Palm, for example. **[0021]** Turning to FIG. 3, an embodiment of a method for controlling access to applications from a mobile device 200 is illustrated with reference to an exemplary message flow scenario. In step 300, the device management server 216 updates the policy database 212 when new applications or services are introduced by the network operator or pursuant to setting up a new customer account. In step 302, when the user requests to launch a video streaming application 206, the application 206 registers with the application manager 210 by providing it with its name and/or type information, such as “Windows Media Player”/“video streaming,” for example. This prompts the application manager 2 10 to request and receive the current access condition information from the access network monitor 208, steps 304-306. In this embodiment, the access condition information includes information regarding the current access network, such as roaming status and compatible network access technology. In steps 308-310, based on the received application information, the application manager 210 requests and receives one or more entries from the policy database 212 indicating which access conditions preclude the establishment of an application session for the application 206. In step 312, the application manager allows the user to launch the requested application if the current access conditions do not match any of the entries returned by the policy database 212 that require denial or suspension of access to the application. In this embodiment, upon establishment of the application session, the access network monitor 208 continuously monitors any changes in the current access conditions. Therefore, when, in step 314, the access network monitor 208 detects a change in the access conditions, for example when the mobile device 200 migrates from an EVDO to a CDMA 2000 1X access network overlay, it notifies the application manager

	210 accordingly. Since this change in the access conditions matches an entry received from the policy database 212 requiring denial of access to the application, the application manager 210, in step 316, sends an event to the application 206 ending the current application session by forcing it to quit. *See* Figs. 1, 2 & 3. To the extent Abichandani does not explicitly and/or inherently disclose this element, it would have been obvious in view of the knowledge of a person of ordinary skill in the art in light of Abichandani alone or it would have been obvious to combine Abichandani with one or more prior art references charted in these Invalidity Contentions or identified in the cover document to which this chart is attached.
i. a differential traffic control policy list distinguishing between a first one or more applications resident on the device and a second one or more applications and/or services resident on the device, and	Abichandani discloses this limitation. For example: **[Abstract]** A system and method are described whereby a mobile device controls access to mobile applications based on access conditions associated with a current access network. To prevent mobile applications from running when the access conditions are not suitable, the mobile device includes a policy database used to store a list of access conditions that are inappropriate for launching the installed applications. The access conditions are based on the type of the current access network used by the mobile device for launching or maintaining the requested application session. The access conditions indicate whether the mobile device is currently accessing its home network or roaming on another provider's network. Similarly, the access conditions indicate the type of network access interface used by the current network to provide the data connection necessary to run the requested application. The policy database correlates predetermined actions with the access conditions associated with a given application session. **[0004]** Embodiments of the invention are used to provide a system and method for controlling access to mobile applications from the mobile device based on access conditions associated with a current access network, To prevent one or more applications or services from running when the access conditions are not suitable, the memory of the mobile device includes a policy or application access database, which is used to store a list of access conditions that are inappropriate for launching the installed applications. In embodiments, the access conditions are based on the type of the current access network used by the mobile device for launching or maintaining the requested application session. For example, the access conditions may indicate whether the mobile device is currently accessing its home network or roaming on another provider's network. Similarly, the access conditions may indicate the type of network access interface used by the current network to provide the data connection necessary to run the requested application. The policy database correlates predetermined actions with current status of access conditions associated with a given application session. In one embodiment, when the mobile device accesses a network having an access technology specification with insufficient data handling capabilities for the requested application, the mobile device denies access to the

	data-intensive application or service specified in the policy database. Similarly, to avoid unwanted roaming charges, the mobile device's policy database includes instructions to suspend any scheduled firmware updates via a firmware over the air (FOTA) application until the mobile device returns to its home network. **[0005]** In one aspect of the invention, a method is provided for controlling access to an application, the application capable of running on a mobile device by connecting to an access network, the method comprising registering the application with the mobile device, populating a record on the mobile device, the record specifying one or more conditions for controlling access to the application, the one or more conditions associated with the access network, monitoring the one or more conditions, and controlling access to the application from the mobile device based on the one or more conditions. **[0006]** In another aspect of the invention, a mobile device is provided, the mobile device capable of running an application by connecting to an access network, the mobile device comprising a processor, a wireless interface for connecting to the access network, and a computer readable medium having thereon instructions for registering the application with the mobile device, populating a record on the mobile device, the record specifying one or more conditions for controlling access to the application, the one or more conditions associated with the access network, monitoring the one or more conditions, and controlling access to the application from the mobile device based on the one or more conditions. **[0007]** In still another aspect of the invention, a system is provided for controlling access to an application, the application capable of running on a mobile device by connecting to an access network, the system comprising (a) the mobile device capable of storing a record for specifying one or more conditions for controlling access to the application, the one or more conditions associated with the access network, the mobile device comprising an access network monitor module configured to monitor the one or more conditions, and an application manager module configured to control access to the application from the mobile device based on the one or more conditions reported by the access network monitor module, and (b) a device management server having a management connection to the mobile device for populating the record. **[0013]** Turning to FIG. 1, an implementation of a system contemplated by an embodiment of the invention is shown with reference to a mobile network environment. In the illustrated embodiment, the user device 100 is a mobile device, such as a wireless telephone or a portable computer capable of launching an application by connecting to an application server 106 via one or more access networks 102, 104. The application server 106 is responsible for content delivery to the one or more applications running on a mobile device 100. For example, when the mobile device 100 includes a multimedia streaming application, the application server 106 employs a Real-Time Transfer Protocol (RTP) to stream the requested content to the multimedia streaming application launched on the mobile device 100. In this embodiment, the application server 106 is part of a core

	network 108, which is an IP Multimedia Services (IMS) network responsible for session control and Quality of Service (QoS) management of ongoing application sessions. Alternately, the application server 106 is located outside of the core network 108, whereby the core network 108 connects to the application server 106 via the Internet 110. In embodiments where the IMS core network 108 is not implemented, the application server 106 may be part of one of the access networks 102, 104, for example, or it may connect to the access networks 102, 104 via the Internet 110. **[0014]** As illustrated in FIG. 1, the access networks 102, 104 interface with the mobile device 100 in accordance with a network interface specification 112. Preferably, the network interface specification 112 complies with one or more wireless access standards, each having corresponding data handling capabilities, such as average and maximum uplink/downlink throughput speeds. In embodiments, the wireless network standards include CDMA 2000 1X, 1xEV-DO, 1xEV-DV, EDGE, and HSPDA network technologies, or combinations thereof In order to launch the application 106, the mobile device 100 typically accesses its home network 102. However, when the access network 102 is not available, such as when the mobile device 100 travels outside of its home coverage area, the mobile device 100 is capable of launching the application 106 via a roaming network 104. **[0015]** Turning to FIG. 2, embodiments of the mobile device 200 and networks 214, 220 are provided in accordance with an embodiment of the present invention, wherein the mobile device 200 controls access to one or more applications 202-206 based on access conditions associated with the access networks 214, 220. The mobile device 200 is capable of launching one or more applications 202-206 from its memory. The applications 202-206 include multimedia, voice, email, instant messaging, text messaging, firmware update, or any other applications or services requiring access to the home network 214 or roaming network 220 to establish an application session. In the illustrated embodiment, the memory of the mobile device 200 includes a Firmware Update Over the Air (FOTA) application 202, a Voice over IP (VoIP) application 204, and a video streaming application 206. **[0016]** To prevent one or more applications or services 202-206 from running when the access conditions are not suitable, the memory of the mobile device 200 includes a policy or application access database 212, which is used to store a list of access conditions that are inappropriate for launching the applications 202-206. Specifically, the access conditions are based on the type of the current access network used by the mobile device 200 for launching or maintaining the requested application session 202-206. For example, the access conditions may indicate whether the mobile device is currently accessing its home network 214 or roaming on the network 220. Similarly, the access conditions may indicate the type of network access interface or standard used by the current network 214, 220 to provide data connection necessary to run the application 202-206. The following table illustrates an example of the policy database 212 having a list of applications and

	corresponding access conditions, which in this embodiment are designated as inappropriate for allowing access to the listed applications or services. **[0017]** Alternatively, the database 212 may contain a list of application/access condition pairs under which access to the requested applications or services is allowed. In embodiments, the policy database 212 includes application types, such as "video streaming" and/or associated application names, such as "Windows Media Player," for example. As illustrated above, the policy database 212 correlates predetermined actions with current status of access conditions associated with a given application session. When the mobile device 200 registers with an access network having a network access technology specification 222 with insufficient data handling capabilities for the requested application, the mobile device 200 is instructed to deny access to a data-intensive application or service specified in the database or lookup table 212. For example, the mobile device 200 is instructed to deny access to a video streaming or VoIP application session when the access conditions indicate that the mobile device 200 is currently using a CDMA 2000 1x network access technology. This avoids unnecessary use of network resources which, under current access conditions, are incapable of providing a satisfying user experience for the desired application. On the other hand, if the current access conditions do not match those in the policy database 212, such as when the mobile device 200 is registered with an EVDO access network, a user is granted full access to the desired video streaming or VoIP applications. Similarly, to avoid unwanted roaming charges, the policy database 212 includes instructions to suspend any scheduled firmware updates via a FOTA application until the mobile device 200 returns to the home network 214. **[0018]** Preferably, the policy database 212 is populated by a network provider using conventional Over the Air Device Management (OTA DM) technology to provide the network operator with full control over the contents of the database 212. In an embodiment, the policy database 212 is centrally populated, distributed, and updated over the air for each mobile device 200 via a management console 218 connected to a device management server 216. The network provider may choose to distribute the policy database 212 according to different classes of mobile devices 200, wherein each device class designates the types of access networks accessible to the device 200, as well as the types of applications installed in its memory. The management console 218, as well as the device management server 216, are located within the home access network 214 or may be collocated with the network administration equipment at a network operations center (NOC) or at a mobile switching center (MSC), for example. **[0019]** As further illustrated in FIG. 2, to gain access to the network resources, the application 202-206 registers with an application manager 210. Specifically, when a user attempts to launch an application 202-206, the application 202-206 supplies its name and/or type information to the application manager 210, which, in turn, receives an input of the monitored access conditions from the access network monitor 208. The

	application manager 210 queries the policy database 212 for the corresponding application/access condition entry and denies access to the application if a match is found. Otherwise, the mobile device 200 initiates the application session over the current access network 214, 220. In a further embodiment, the access network monitor 208 continues to report the changes in current access conditions during the application session to allow the application manager 210 to terminate the application when a change in the access conditions matches an entry in the policy database 212. **[0020]** In this embodiment, the application manager 210 and the access network monitor 208 are implemented as Binary Runtime Environment for Wireless (BREW) software modules exposing standard interfaces for interaction with other software components of the mobile device 200 via an application programming interface (API). Other embodiments of the application manager 210 and access network monitor 208 include using a Java-based implementation capable of running on a plurality of mobile phone operating systems, such as Symbian, Windows Mobile Edition, or Palm, for example. **[0021]** Turning to FIG. 3, an embodiment of a method for controlling access to applications from a mobile device 200 is illustrated with reference to an exemplary message flow scenario. In step 300, the device management server 216 updates the policy database 212 when new applications or services are introduced by the network operator or pursuant to setting up a new customer account. In step 302, when the user requests to launch a video streaming application 206, the application 206 registers with the application manager 210 by providing it with its name and/or type information, such as “Windows Media Player”/“video streaming,” for example. This prompts the application manager 2 10 to request and receive the current access condition information from the access network monitor 208, steps 304-306. In this embodiment, the access condition information includes information regarding the current access network, such as roaming status and compatible network access technology. In steps 308-310, based on the received application information, the application manager 210 requests and receives one or more entries from the policy database 212 indicating which access conditions preclude the establishment of an application session for the application 206. In step 312, the application manager allows the user to launch the requested application if the current access conditions do not match any of the entries returned by the policy database 212 that require denial or suspension of access to the application. In this embodiment, upon establishment of the application session, the access network monitor 208 continuously monitors any changes in the current access conditions. Therefore, when, in step 314, the access network monitor 208 detects a change in the access conditions, for example when the mobile device 200 migrates from an EVDO to a CDMA 2000 1X access network overlay, it notifies the application manager 210 accordingly. Since this change in the access conditions matches an entry received from the policy database 212 requiring denial of access to the application, the application manager 210, in step 316, sends an event to the application 206 ending the current application session by forcing it to quit.

	See Figs. 1, 2 & 3. To the extent Abichandani does not explicitly and/or inherently disclose this element, it would have been obvious in view of the knowledge of a person of ordinary skill in the art in light of Abichandani alone or it would have been obvious to combine Abichandani with one or more prior art references charted in these Invalidity Contentions or identified in the cover document to which this chart is attached.
ii. a differential traffic control policy applicable to at least some Internet service activities by or on behalf of the first one or more applications;	Abichandani discloses this limitation. For example: **[Abstract]** A system and method are described whereby a mobile device controls access to mobile applications based on access conditions associated with a current access network. To prevent mobile applications from running when the access conditions are not suitable, the mobile device includes a policy database used to store a list of access conditions that are inappropriate for launching the installed applications. The access conditions are based on the type of the current access network used by the mobile device for launching or maintaining the requested application session. The access conditions indicate whether the mobile device is currently accessing its home network or roaming on another provider's network. Similarly, the access conditions indicate the type of network access interface used by the current network to provide the data connection necessary to run the requested application. The policy database correlates predetermined actions with the access conditions associated with a given application session. **[0004]** Embodiments of the invention are used to provide a system and method for controlling access to mobile applications from the mobile device based on access conditions associated with a current access network, To prevent one or more applications or services from running when the access conditions are not suitable, the memory of the mobile device includes a policy or application access database, which is used to store a list of access conditions that are inappropriate for launching the installed applications. In embodiments, the access conditions are based on the type of the current access network used by the mobile device for launching or maintaining the requested application session. For example, the access conditions may indicate whether the mobile device is currently accessing its home network or roaming on another provider's network. Similarly, the access conditions may indicate the type of network access interface used by the current network to provide the data connection necessary to run the requested application. The policy database correlates predetermined actions with current status of access conditions associated with a given application session. In one embodiment, when the mobile device accesses a network having an access technology specification with insufficient data handling capabilities for the requested application, the mobile device denies access to the data-intensive application or service specified in the policy database. Similarly, to avoid unwanted roaming charges, the mobile device's policy database includes instructions to suspend any scheduled firmware updates via a firmware over the air (FOTA) application until the mobile device returns to its home network.

	[0005] In one aspect of the invention, a method is provided for controlling access to an application, the application capable of running on a mobile device by connecting to an access network, the method comprising registering the application with the mobile device, populating a record on the mobile device, the record specifying one or more conditions for controlling access to the application, the one or more conditions associated with the access network, monitoring the one or more conditions, and controlling access to the application from the mobile device based on the one or more conditions. **[0006]** In another aspect of the invention, a mobile device is provided, the mobile device capable of running an application by connecting to an access network, the mobile device comprising a processor, a wireless interface for connecting to the access network, and a computer readable medium having thereon instructions for registering the application with the mobile device, populating a record on the mobile device, the record specifying one or more conditions for controlling access to the application, the one or more conditions associated with the access network, monitoring the one or more conditions, and controlling access to the application from the mobile device based on the one or more conditions. **[0007]** In still another aspect of the invention, a system is provided for controlling access to an application, the application capable of running on a mobile device by connecting to an access network, the system comprising (a) the mobile device capable of storing a record for specifying one or more conditions for controlling access to the application, the one or more conditions associated with the access network, the mobile device comprising an access network monitor module configured to monitor the one or more conditions, and an application manager module configured to control access to the application from the mobile device based on the one or more conditions reported by the access network monitor module, and (b) a device management server having a management connection to the mobile device for populating the record. **[0013]** Turning to FIG. 1, an implementation of a system contemplated by an embodiment of the invention is shown with reference to a mobile network environment. In the illustrated embodiment, the user device 100 is a mobile device, such as a wireless telephone or a portable computer capable of launching an application by connecting to an application server 106 via one or more access networks 102, 104. The application server 106 is responsible for content delivery to the one or more applications running on a mobile device 100. For example, when the mobile device 100 includes a multimedia streaming application, the application server 106 employs a Real-Time Transfer Protocol (RTP) to stream the requested content to the multimedia streaming application launched on the mobile device 100. In this embodiment, the application server 106 is part of a core network 108, which is an IP Multimedia Services (IMS) network responsible for session control and Quality of Service (QoS) management of ongoing application sessions. Alternately, the application server 106 is located outside of the core network 108, whereby the core network 108 connects to the application server 106 via the Internet 110. In embodiments where the IMS core network 108 is not implemented, the application

	server 106 may be part of one of the access networks 102, 104, for example, or it may connect to the access networks 102, 104 via the Internet 110. **[0014]** As illustrated in FIG. 1, the access networks 102, 104 interface with the mobile device 100 in accordance with a network interface specification 112. Preferably, the network interface specification 112 complies with one or more wireless access standards, each having corresponding data handling capabilities, such as average and maximum uplink/downlink throughput speeds. In embodiments, the wireless network standards include CDMA 2000 1X, 1xEV-DO, 1xEV-DV, EDGE, and HSPDA network technologies, or combinations thereof In order to launch the application 106, the mobile device 100 typically accesses its home network 102. However, when the access network 102 is not available, such as when the mobile device 100 travels outside of its home coverage area, the mobile device 100 is capable of launching the application 106 via a roaming network 104. **[0015]** Turning to FIG. 2, embodiments of the mobile device 200 and networks 214, 220 are provided in accordance with an embodiment of the present invention, wherein the mobile device 200 controls access to one or more applications 202-206 based on access conditions associated with the access networks 214, 220. The mobile device 200 is capable of launching one or more applications 202-206 from its memory. The applications 202-206 include multimedia, voice, email, instant messaging, text messaging, firmware update, or any other applications or services requiring access to the home network 214 or roaming network 220 to establish an application session. In the illustrated embodiment, the memory of the mobile device 200 includes a Firmware Update Over the Air (FOTA) application 202, a Voice over IP (VoIP) application 204, and a video streaming application 206. **[0016]** To prevent one or more applications or services 202-206 from running when the access conditions are not suitable, the memory of the mobile device 200 includes a policy or application access database 212, which is used to store a list of access conditions that are inappropriate for launching the applications 202-206. Specifically, the access conditions are based on the type of the current access network used by the mobile device 200 for launching or maintaining the requested application session 202-206. For example, the access conditions may indicate whether the mobile device is currently accessing its home network 214 or roaming on the network 220. Similarly, the access conditions may indicate the type of network access interface or standard used by the current network 214, 220 to provide data connection necessary to run the application 202-206. The following table illustrates an example of the policy database 212 having a list of applications and corresponding access conditions, which in this embodiment are designated as inappropriate for allowing access to the listed applications or services. **[0017]** Alternatively, the database 212 may contain a list of application/access condition pairs under which access to the requested applications or services is allowed. In embodiments, the policy database 212 includes

	application types, such as "video streaming" and/or associated application names, such as "Windows Media Player," for example. As illustrated above, the policy database 212 correlates predetermined actions with current status of access conditions associated with a given application session. When the mobile device 200 registers with an access network having a network access technology specification 222 with insufficient data handling capabilities for the requested application, the mobile device 200 is instructed to deny access to a data-intensive application or service specified in the database or lookup table 212. For example, the mobile device 200 is instructed to deny access to a video streaming or VoIP application session when the access conditions indicate that the mobile device 200 is currently using a CDMA 2000 1x network access technology. This avoids unnecessary use of network resources which, under current access conditions, are incapable of providing a satisfying user experience for the desired application. On the other hand, if the current access conditions do not match those in the policy database 212, such as when the mobile device 200 is registered with an EVDO access network, a user is granted full access to the desired video streaming or VoIP applications. Similarly, to avoid unwanted roaming charges, the policy database 212 includes instructions to suspend any scheduled firmware updates via a FOTA application until the mobile device 200 returns to the home network 214. **[0018]** Preferably, the policy database 212 is populated by a network provider using conventional Over the Air Device Management (OTA DM) technology to provide the network operator with full control over the contents of the database 212. In an embodiment, the policy database 212 is centrally populated, distributed, and updated over the air for each mobile device 200 via a management console 218 connected to a device management server 216. The network provider may choose to distribute the policy database 212 according to different classes of mobile devices 200, wherein each device class designates the types of access networks accessible to the device 200, as well as the types of applications installed in its memory. The management console 218, as well as the device management server 216, are located within the home access network 214 or may be collocated with the network administration equipment at a network operations center (NOC) or at a mobile switching center (MSC), for example. **[0019]** As further illustrated in FIG. 2, to gain access to the network resources, the application 202-206 registers with an application manager 210. Specifically, when a user attempts to launch an application 202-206, the application 202-206 supplies its name and/or type information to the application manager 210, which, in turn, receives an input of the monitored access conditions from the access network monitor 208. The application manager 210 queries the policy database 212 for the corresponding application/access condition entry and denies access to the application if a match is found. Otherwise, the mobile device 200 initiates the application session over the current access network 214, 220. In a further embodiment, the access network monitor 208 continues to report the changes in current access conditions during the application session to

	allow the application manager 210 to terminate the application when a change in the access conditions matches an entry in the policy database 212. **[0020]** In this embodiment, the application manager 210 and the access network monitor 208 are implemented as Binary Runtime Environment for Wireless (BREW) software modules exposing standard interfaces for interaction with other software components of the mobile device 200 via an application programming interface (API). Other embodiments of the application manager 210 and access network monitor 208 include using a Java-based implementation capable of running on a plurality of mobile phone operating systems, such as Symbian, Windows Mobile Edition, or Palm, for example. **[0021]** Turning to FIG. 3, an embodiment of a method for controlling access to applications from a mobile device 200 is illustrated with reference to an exemplary message flow scenario. In step 300, the device management server 216 updates the policy database 212 when new applications or services are introduced by the network operator or pursuant to setting up a new customer account. In step 302, when the user requests to launch a video streaming application 206, the application 206 registers with the application manager 210 by providing it with its name and/or type information, such as "Windows Media Player"/"video streaming," for example. This prompts the application manager 2 10 to request and receive the current access condition information from the access network monitor 208, steps 304-306. In this embodiment, the access condition information includes information regarding the current access network, such as roaming status and compatible network access technology. In steps 308-310, based on the received application information, the application manager 210 requests and receives one or more entries from the policy database 212 indicating which access conditions preclude the establishment of an application session for the application 206. In step 312, the application manager allows the user to launch the requested application if the current access conditions do not match any of the entries returned by the policy database 212 that require denial or suspension of access to the application. In this embodiment, upon establishment of the application session, the access network monitor 208 continuously monitors any changes in the current access conditions. Therefore, when, in step 314, the access network monitor 208 detects a change in the access conditions, for example when the mobile device 200 migrates from an EVDO to a CDMA 2000 1X access network overlay, it notifies the application manager 210 accordingly. Since this change in the access conditions matches an entry received from the policy database 212 requiring denial of access to the application, the application manager 210, in step 316, sends an event to the application 206 ending the current application session by forcing it to quit. *See* Figs. 1, 2 & 3. To the extent Abichandani does not explicitly and/or inherently disclose this element, it would have been obvious in view of the knowledge of a person of ordinary skill in the art in light of Abichandani alone or it

	would have been obvious to combine Abichandani with one or more prior art references charted in these Invalidity Contentions or identified in the cover document to which this chart is attached.
(d) an interface to allow a user to augment the differential traffic control policy for the first one or more applications but not for the second one or more applications and/or services; and	Abichandani discloses this limitation. For example: **[Abstract]** A system and method are described whereby a mobile device controls access to mobile applications based on access conditions associated with a current access network. To prevent mobile applications from running when the access conditions are not suitable, the mobile device includes a policy database used to store a list of access conditions that are inappropriate for launching the installed applications. The access conditions are based on the type of the current access network used by the mobile device for launching or maintaining the requested application session. The access conditions indicate whether the mobile device is currently accessing its home network or roaming on another provider's network. Similarly, the access conditions indicate the type of network access interface used by the current network to provide the data connection necessary to run the requested application. The policy database correlates predetermined actions with the access conditions associated with a given application session. **[0004]** Embodiments of the invention are used to provide a system and method for controlling access to mobile applications from the mobile device based on access conditions associated with a current access network, To prevent one or more applications or services from running when the access conditions are not suitable, the memory of the mobile device includes a policy or application access database, which is used to store a list of access conditions that are inappropriate for launching the installed applications. In embodiments, the access conditions are based on the type of the current access network used by the mobile device for launching or maintaining the requested application session. For example, the access conditions may indicate whether the mobile device is currently accessing its home network or roaming on another provider's network. Similarly, the access conditions may indicate the type of network access interface used by the current network to provide the data connection necessary to run the requested application. The policy database correlates predetermined actions with current status of access conditions associated with a given application session. In one embodiment, when the mobile device accesses a network having an access technology specification with insufficient data handling capabilities for the requested application, the mobile device denies access to the data-intensive application or service specified in the policy database. Similarly, to avoid unwanted roaming charges, the mobile device's policy database includes instructions to suspend any scheduled firmware updates via a firmware over the air (FOTA) application until the mobile device returns to its home network. **[0005]** In one aspect of the invention, a method is provided for controlling access to an application, the application capable of running on a mobile device by connecting to an access network, the method comprising registering the application with the mobile device, populating a record on the mobile device, the record specifying one or more conditions for controlling access to the application, the one or more conditions

	associated with the access network, monitoring the one or more conditions, and controlling access to the application from the mobile device based on the one or more conditions. **[0006]** In another aspect of the invention, a mobile device is provided, the mobile device capable of running an application by connecting to an access network, the mobile device comprising a processor, a wireless interface for connecting to the access network, and a computer readable medium having thereon instructions for registering the application with the mobile device, populating a record on the mobile device, the record specifying one or more conditions for controlling access to the application, the one or more conditions associated with the access network, monitoring the one or more conditions, and controlling access to the application from the mobile device based on the one or more conditions. **[0007]** In still another aspect of the invention, a system is provided for controlling access to an application, the application capable of running on a mobile device by connecting to an access network, the system comprising (a) the mobile device capable of storing a record for specifying one or more conditions for controlling access to the application, the one or more conditions associated with the access network, the mobile device comprising an access network monitor module configured to monitor the one or more conditions, and an application manager module configured to control access to the application from the mobile device based on the one or more conditions reported by the access network monitor module, and (b) a device management server having a management connection to the mobile device for populating the record. **[0013]** Turning to FIG. 1, an implementation of a system contemplated by an embodiment of the invention is shown with reference to a mobile network environment. In the illustrated embodiment, the user device 100 is a mobile device, such as a wireless telephone or a portable computer capable of launching an application by connecting to an application server 106 via one or more access networks 102, 104. The application server 106 is responsible for content delivery to the one or more applications running on a mobile device 100. For example, when the mobile device 100 includes a multimedia streaming application, the application server 106 employs a Real-Time Transfer Protocol (RTP) to stream the requested content to the multimedia streaming application launched on the mobile device 100. In this embodiment, the application server 106 is part of a core network 108, which is an IP Multimedia Services (IMS) network responsible for session control and Quality of Service (QoS) management of ongoing application sessions. Alternately, the application server 106 is located outside of the core network 108, whereby the core network 108 connects to the application server 106 via the Internet 110. In embodiments where the IMS core network 108 is not implemented, the application server 106 may be part of one of the access networks 102, 104, for example, or it may connect to the access networks 102, 104 via the Internet 110.

	[0014] As illustrated in FIG. 1, the access networks 102, 104 interface with the mobile device 100 in accordance with a network interface specification 112. Preferably, the network interface specification 112 complies with one or more wireless access standards, each having corresponding data handling capabilities, such as average and maximum uplink/downlink throughput speeds. In embodiments, the wireless network standards include CDMA 2000 1X, 1xEV-DO, 1xEV-DV, EDGE, and HSPDA network technologies, or combinations thereof In order to launch the application 106, the mobile device 100 typically accesses its home network 102. However, when the access network 102 is not available, such as when the mobile device 100 travels outside of its home coverage area, the mobile device 100 is capable of launching the application 106 via a roaming network 104. **[0015]** Turning to FIG. 2, embodiments of the mobile device 200 and networks 214, 220 are provided in accordance with an embodiment of the present invention, wherein the mobile device 200 controls access to one or more applications 202-206 based on access conditions associated with the access networks 214, 220. The mobile device 200 is capable of launching one or more applications 202-206 from its memory. The applications 202-206 include multimedia, voice, email, instant messaging, text messaging, firmware update, or any other applications or services requiring access to the home network 214 or roaming network 220 to establish an application session. In the illustrated embodiment, the memory of the mobile device 200 includes a Firmware Update Over the Air (FOTA) application 202, a Voice over IP (VoIP) application 204, and a video streaming application 206. **[0016]** To prevent one or more applications or services 202-206 from running when the access conditions are not suitable, the memory of the mobile device 200 includes a policy or application access database 212, which is used to store a list of access conditions that are inappropriate for launching the applications 202-206. Specifically, the access conditions are based on the type of the current access network used by the mobile device 200 for launching or maintaining the requested application session 202-206. For example, the access conditions may indicate whether the mobile device is currently accessing its home network 214 or roaming on the network 220. Similarly, the access conditions may indicate the type of network access interface or standard used by the current network 214, 220 to provide data connection necessary to run the application 202-206. The following table illustrates an example of the policy database 212 having a list of applications and corresponding access conditions, which in this embodiment are designated as inappropriate for allowing access to the listed applications or services. **[0017]** Alternatively, the database 212 may contain a list of application/access condition pairs under which access to the requested applications or services is allowed. In embodiments, the policy database 212 includes application types, such as “video streaming” and/or associated application names, such as “Windows Media Player,” for example. As illustrated above, the policy database 212 correlates predetermined actions with current status of access conditions associated with a given application session. When the mobile device 200

	registers with an access network having a network access technology specification 222 with insufficient data handling capabilities for the requested application, the mobile device 200 is instructed to deny access to a data-intensive application or service specified in the database or lookup table 212. For example, the mobile device 200 is instructed to deny access to a video streaming or VoIP application session when the access conditions indicate that the mobile device 200 is currently using a CDMA 2000 1x network access technology. This avoids unnecessary use of network resources which, under current access conditions, are incapable of providing a satisfying user experience for the desired application. On the other hand, if the current access conditions do not match those in the policy database 212, such as when the mobile device 200 is registered with an EVDO access network, a user is granted full access to the desired video streaming or VoIP applications. Similarly, to avoid unwanted roaming charges, the policy database 212 includes instructions to suspend any scheduled firmware updates via a FOTA application until the mobile device 200 returns to the home network 214. **[0018]** Preferably, the policy database 212 is populated by a network provider using conventional Over the Air Device Management (OTA DM) technology to provide the network operator with full control over the contents of the database 212. In an embodiment, the policy database 212 is centrally populated, distributed, and updated over the air for each mobile device 200 via a management console 218 connected to a device management server 216. The network provider may choose to distribute the policy database 212 according to different classes of mobile devices 200, wherein each device class designates the types of access networks accessible to the device 200, as well as the types of applications installed in its memory. The management console 218, as well as the device management server 216, are located within the home access network 214 or may be collocated with the network administration equipment at a network operations center (NOC) or at a mobile switching center (MSC), for example. **[0019]** As further illustrated in FIG. 2, to gain access to the network resources, the application 202-206 registers with an application manager 210. Specifically, when a user attempts to launch an application 202-206, the application 202-206 supplies its name and/or type information to the application manager 210, which, in turn, receives an input of the monitored access conditions from the access network monitor 208. The application manager 210 queries the policy database 212 for the corresponding application/access condition entry and denies access to the application if a match is found. Otherwise, the mobile device 200 initiates the application session over the current access network 214, 220. In a further embodiment, the access network monitor 208 continues to report the changes in current access conditions during the application session to allow the application manager 210 to terminate the application when a change in the access conditions matches an entry in the policy database 212.

	[0020] In this embodiment, the application manager 210 and the access network monitor 208 are implemented as Binary Runtime Environment for Wireless (BREW) software modules exposing standard interfaces for interaction with other software components of the mobile device 200 via an application programming interface (API). Other embodiments of the application manager 210 and access network monitor 208 include using a Java-based implementation capable of running on a plurality of mobile phone operating systems, such as Symbian, Windows Mobile Edition, or Palm, for example. **[0021]** Turning to FIG. 3, an embodiment of a method for controlling access to applications from a mobile device 200 is illustrated with reference to an exemplary message flow scenario. In step 300, the device management server 216 updates the policy database 212 when new applications or services are introduced by the network operator or pursuant to setting up a new customer account. In step 302, when the user requests to launch a video streaming application 206, the application 206 registers with the application manager 210 by providing it with its name and/or type information, such as "Windows Media Player"/"video streaming," for example. This prompts the application manager 2 10 to request and receive the current access condition information from the access network monitor 208, steps 304-306. In this embodiment, the access condition information includes information regarding the current access network, such as roaming status and compatible network access technology. In steps 308-310, based on the received application information, the application manager 210 requests and receives one or more entries from the policy database 212 indicating which access conditions preclude the establishment of an application session for the application 206. In step 312, the application manager allows the user to launch the requested application if the current access conditions do not match any of the entries returned by the policy database 212 that require denial or suspension of access to the application. In this embodiment, upon establishment of the application session, the access network monitor 208 continuously monitors any changes in the current access conditions. Therefore, when, in step 314, the access network monitor 208 detects a change in the access conditions, for example when the mobile device 200 migrates from an EVDO to a CDMA 2000 1X access network overlay, it notifies the application manager 210 accordingly. Since this change in the access conditions matches an entry received from the policy database 212 requiring denial of access to the application, the application manager 210, in step 316, sends an event to the application 206 ending the current application session by forcing it to quit. *See* Figs. 1, 2 & 3. To the extent Abichandani does not explicitly and/or inherently disclose this element, it would have been obvious in view of the knowledge of a person of ordinary skill in the art in light of Abichandani alone or it would have been obvious to combine Abichandani with one or more prior art references charted in these Invalidity Contentions or identified in the cover document to which this chart is attached.
(e) one or more processors configured to	Abichandani discloses this limitation. For example:

	[Abstract] A system and method are described whereby a mobile device controls access to mobile applications based on access conditions associated with a current access network. To prevent mobile applications from running when the access conditions are not suitable, the mobile device includes a policy database used to store a list of access conditions that are inappropriate for launching the installed applications. The access conditions are based on the type of the current access network used by the mobile device for launching or maintaining the requested application session. The access conditions indicate whether the mobile device is currently accessing its home network or roaming on another provider's network. Similarly, the access conditions indicate the type of network access interface used by the current network to provide the data connection necessary to run the requested application. The policy database correlates predetermined actions with the access conditions associated with a given application session. **[0004]** Embodiments of the invention are used to provide a system and method for controlling access to mobile applications from the mobile device based on access conditions associated with a current access network, To prevent one or more applications or services from running when the access conditions are not suitable, the memory of the mobile device includes a policy or application access database, which is used to store a list of access conditions that are inappropriate for launching the installed applications. In embodiments, the access conditions are based on the type of the current access network used by the mobile device for launching or maintaining the requested application session. For example, the access conditions may indicate whether the mobile device is currently accessing its home network or roaming on another provider's network. Similarly, the access conditions may indicate the type of network access interface used by the current network to provide the data connection necessary to run the requested application. The policy database correlates predetermined actions with current status of access conditions associated with a given application session. In one embodiment, when the mobile device accesses a network having an access technology specification with insufficient data handling capabilities for the requested application, the mobile device denies access to the data-intensive application or service specified in the policy database. Similarly, to avoid unwanted roaming charges, the mobile device's policy database includes instructions to suspend any scheduled firmware updates via a firmware over the air (FOTA) application until the mobile device returns to its home network. **[0005]** In one aspect of the invention, a method is provided for controlling access to an application, the application capable of running on a mobile device by connecting to an access network, the method comprising registering the application with the mobile device, populating a record on the mobile device, the record specifying one or more conditions for controlling access to the application, the one or more conditions associated with the access network, monitoring the one or more conditions, and controlling access to the application from the mobile device based on the one or more conditions.

	[0006] In another aspect of the invention, a mobile device is provided, the mobile device capable of running an application by connecting to an access network, the mobile device comprising a processor, a wireless interface for connecting to the access network, and a computer readable medium having thereon instructions for registering the application with the mobile device, populating a record on the mobile device, the record specifying one or more conditions for controlling access to the application, the one or more conditions associated with the access network, monitoring the one or more conditions, and controlling access to the application from the mobile device based on the one or more conditions. **[0007]** In still another aspect of the invention, a system is provided for controlling access to an application, the application capable of running on a mobile device by connecting to an access network, the system comprising (a) the mobile device capable of storing a record for specifying one or more conditions for controlling access to the application, the one or more conditions associated with the access network, the mobile device comprising an access network monitor module configured to monitor the one or more conditions, and an application manager module configured to control access to the application from the mobile device based on the one or more conditions reported by the access network monitor module, and (b) a device management server having a management connection to the mobile device for populating the record. **[0013]** Turning to FIG. 1, an implementation of a system contemplated by an embodiment of the invention is shown with reference to a mobile network environment. In the illustrated embodiment, the user device 100 is a mobile device, such as a wireless telephone or a portable computer capable of launching an application by connecting to an application server 106 via one or more access networks 102, 104. The application server 106 is responsible for content delivery to the one or more applications running on a mobile device 100. For example, when the mobile device 100 includes a multimedia streaming application, the application server 106 employs a Real-Time Transfer Protocol (RTP) to stream the requested content to the multimedia streaming application launched on the mobile device 100. In this embodiment, the application server 106 is part of a core network 108, which is an IP Multimedia Services (IMS) network responsible for session control and Quality of Service (QoS) management of ongoing application sessions. Alternately, the application server 106 is located outside of the core network 108, whereby the core network 108 connects to the application server 106 via the Internet 110. In embodiments where the IMS core network 108 is not implemented, the application server 106 may be part of one of the access networks 102, 104, for example, or it may connect to the access networks 102, 104 via the Internet 110. **[0014]** As illustrated in FIG. 1, the access networks 102, 104 interface with the mobile device 100 in accordance with a network interface specification 112. Preferably, the network interface specification 112 complies with one or more wireless access standards, each having corresponding data handling capabilities, such as average and maximum uplink/downlink throughput speeds. In embodiments, the wireless network

	standards include CDMA 2000 1X, 1xEV-DO, 1xEV-DV, EDGE, and HSPDA network technologies, or combinations thereof In order to launch the application 106, the mobile device 100 typically accesses its home network 102. However, when the access network 102 is not available, such as when the mobile device 100 travels outside of its home coverage area, the mobile device 100 is capable of launching the application 106 via a roaming network 104. **[0015]** Turning to FIG. 2, embodiments of the mobile device 200 and networks 214, 220 are provided in accordance with an embodiment of the present invention, wherein the mobile device 200 controls access to one or more applications 202-206 based on access conditions associated with the access networks 214, 220. The mobile device 200 is capable of launching one or more applications 202-206 from its memory. The applications 202-206 include multimedia, voice, email, instant messaging, text messaging, firmware update, or any other applications or services requiring access to the home network 214 or roaming network 220 to establish an application session. In the illustrated embodiment, the memory of the mobile device 200 includes a Firmware Update Over the Air (FOTA) application 202, a Voice over IP (VoIP) application 204, and a video streaming application 206. **[0016]** To prevent one or more applications or services 202-206 from running when the access conditions are not suitable, the memory of the mobile device 200 includes a policy or application access database 212, which is used to store a list of access conditions that are inappropriate for launching the applications 202-206. Specifically, the access conditions are based on the type of the current access network used by the mobile device 200 for launching or maintaining the requested application session 202-206. For example, the access conditions may indicate whether the mobile device is currently accessing its home network 214 or roaming on the network 220. Similarly, the access conditions may indicate the type of network access interface or standard used by the current network 214, 220 to provide data connection necessary to run the application 202-206. The following table illustrates an example of the policy database 212 having a list of applications and corresponding access conditions, which in this embodiment are designated as inappropriate for allowing access to the listed applications or services. **[0017]** Alternatively, the database 212 may contain a list of application/access condition pairs under which access to the requested applications or services is allowed. In embodiments, the policy database 212 includes application types, such as “video streaming” and/or associated application names, such as “Windows Media Player,” for example. As illustrated above, the policy database 212 correlates predetermined actions with current status of access conditions associated with a given application session. When the mobile device 200 registers with an access network having a network access technology specification 222 with insufficient data handling capabilities for the requested application, the mobile device 200 is instructed to deny access to a data-intensive application or service specified in the database or lookup table 212. For example, the mobile device 200 is instructed to deny access to a video streaming or VoIP application session when the access

	conditions indicate that the mobile device 200 is currently using a CDMA 2000 1x network access technology. This avoids unnecessary use of network resources which, under current access conditions, are incapable of providing a satisfying user experience for the desired application. On the other hand, if the current access conditions do not match those in the policy database 212, such as when the mobile device 200 is registered with an EVDO access network, a user is granted full access to the desired video streaming or VoIP applications. Similarly, to avoid unwanted roaming charges, the policy database 212 includes instructions to suspend any scheduled firmware updates via a FOTA application until the mobile device 200 returns to the home network 214. **[0018]** Preferably, the policy database 212 is populated by a network provider using conventional Over the Air Device Management (OTA DM) technology to provide the network operator with full control over the contents of the database 212. In an embodiment, the policy database 212 is centrally populated, distributed, and updated over the air for each mobile device 200 via a management console 218 connected to a device management server 216. The network provider may choose to distribute the policy database 212 according to different classes of mobile devices 200, wherein each device class designates the types of access networks accessible to the device 200, as well as the types of applications installed in its memory. The management console 218, as well as the device management server 216, are located within the home access network 214 or may be collocated with the network administration equipment at a network operations center (NOC) or at a mobile switching center (MSC), for example. **[0019]** As further illustrated in FIG. 2, to gain access to the network resources, the application 202-206 registers with an application manager 210. Specifically, when a user attempts to launch an application 202-206, the application 202-206 supplies its name and/or type information to the application manager 210, which, in turn, receives an input of the monitored access conditions from the access network monitor 208. The application manager 210 queries the policy database 212 for the corresponding application/access condition entry and denies access to the application if a match is found. Otherwise, the mobile device 200 initiates the application session over the current access network 214, 220. In a further embodiment, the access network monitor 208 continues to report the changes in current access conditions during the application session to allow the application manager 210 to terminate the application when a change in the access conditions matches an entry in the policy database 212. **[0020]** In this embodiment, the application manager 210 and the access network monitor 208 are implemented as Binary Runtime Environment for Wireless (BREW) software modules exposing standard interfaces for interaction with other software components of the mobile device 200 via an application programming interface (API). Other embodiments of the application manager 210 and access network monitor 208 include using a

	Java-based implementation capable of running on a plurality of mobile phone operating systems, such as Symbian, Windows Mobile Edition, or Palm, for example. **[0021]** Turning to FIG. 3, an embodiment of a method for controlling access to applications from a mobile device 200 is illustrated with reference to an exemplary message flow scenario. In step 300, the device management server 216 updates the policy database 212 when new applications or services are introduced by the network operator or pursuant to setting up a new customer account. In step 302, when the user requests to launch a video streaming application 206, the application 206 registers with the application manager 210 by providing it with its name and/or type information, such as "Windows Media Player"/"video streaming," for example. This prompts the application manager 2 10 to request and receive the current access condition information from the access network monitor 208, steps 304-306. In this embodiment, the access condition information includes information regarding the current access network, such as roaming status and compatible network access technology. In steps 308-310, based on the received application information, the application manager 210 requests and receives one or more entries from the policy database 212 indicating which access conditions preclude the establishment of an application session for the application 206. In step 312, the application manager allows the user to launch the requested application if the current access conditions do not match any of the entries returned by the policy database 212 that require denial or suspension of access to the application. In this embodiment, upon establishment of the application session, the access network monitor 208 continuously monitors any changes in the current access conditions. Therefore, when, in step 314, the access network monitor 208 detects a change in the access conditions, for example when the mobile device 200 migrates from an EVDO to a CDMA 2000 1X access network overlay, it notifies the application manager 210 accordingly. Since this change in the access conditions matches an entry received from the policy database 212 requiring denial of access to the application, the application manager 210, in step 316, sends an event to the application 206 ending the current application session by forcing it to quit. *See* Figs. 1, 2 & 3. To the extent Abichandani does not explicitly and/or inherently disclose this element, it would have been obvious in view of the knowledge of a person of ordinary skill in the art in light of Abichandani alone or it would have been obvious to combine Abichandani with one or more prior art references charted in these Invalidity Contentions or identified in the cover document to which this chart is attached.
i. classify a wireless network to which the device currently connects in order to communicate data for Internet service activities as at least one of a plurality of	Abichandani discloses this limitation. For example: **[Abstract]** A system and method are described whereby a mobile device controls access to mobile applications based on access conditions associated with a current access network. To prevent mobile applications from running when the access conditions are not suitable, the mobile device includes a policy

network types that the device can connect with,	database used to store a list of access conditions that are inappropriate for launching the installed applications. The access conditions are based on the type of the current access network used by the mobile device for launching or maintaining the requested application session. The access conditions indicate whether the mobile device is currently accessing its home network or roaming on another provider's network. Similarly, the access conditions indicate the type of network access interface used by the current network to provide the data connection necessary to run the requested application. The policy database correlates predetermined actions with the access conditions associated with a given application session. **[0004]** Embodiments of the invention are used to provide a system and method for controlling access to mobile applications from the mobile device based on access conditions associated with a current access network, To prevent one or more applications or services from running when the access conditions are not suitable, the memory of the mobile device includes a policy or application access database, which is used to store a list of access conditions that are inappropriate for launching the installed applications. In embodiments, the access conditions are based on the type of the current access network used by the mobile device for launching or maintaining the requested application session. For example, the access conditions may indicate whether the mobile device is currently accessing its home network or roaming on another provider's network. Similarly, the access conditions may indicate the type of network access interface used by the current network to provide the data connection necessary to run the requested application. The policy database correlates predetermined actions with current status of access conditions associated with a given application session. In one embodiment, when the mobile device accesses a network having an access technology specification with insufficient data handling capabilities for the requested application, the mobile device denies access to the data-intensive application or service specified in the policy database. Similarly, to avoid unwanted roaming charges, the mobile device's policy database includes instructions to suspend any scheduled firmware updates via a firmware over the air (FOTA) application until the mobile device returns to its home network. **[0005]** In one aspect of the invention, a method is provided for controlling access to an application, the application capable of running on a mobile device by connecting to an access network, the method comprising registering the application with the mobile device, populating a record on the mobile device, the record specifying one or more conditions for controlling access to the application, the one or more conditions associated with the access network, monitoring the one or more conditions, and controlling access to the application from the mobile device based on the one or more conditions. **[0006]** In another aspect of the invention, a mobile device is provided, the mobile device capable of running an application by connecting to an access network, the mobile device comprising a processor, a wireless interface for connecting to the access network, and a computer readable medium having thereon instructions for registering the application with the mobile device, populating a record on the mobile device, the record

	specifying one or more conditions for controlling access to the application, the one or more conditions associated with the access network, monitoring the one or more conditions, and controlling access to the application from the mobile device based on the one or more conditions. **[0007]** In still another aspect of the invention, a system is provided for controlling access to an application, the application capable of running on a mobile device by connecting to an access network, the system comprising (a) the mobile device capable of storing a record for specifying one or more conditions for controlling access to the application, the one or more conditions associated with the access network, the mobile device comprising an access network monitor module configured to monitor the one or more conditions, and an application manager module configured to control access to the application from the mobile device based on the one or more conditions reported by the access network monitor module, and (b) a device management server having a management connection to the mobile device for populating the record. **[0013]** Turning to FIG. 1, an implementation of a system contemplated by an embodiment of the invention is shown with reference to a mobile network environment. In the illustrated embodiment, the user device 100 is a mobile device, such as a wireless telephone or a portable computer capable of launching an application by connecting to an application server 106 via one or more access networks 102, 104. The application server 106 is responsible for content delivery to the one or more applications running on a mobile device 100. For example, when the mobile device 100 includes a multimedia streaming application, the application server 106 employs a Real-Time Transfer Protocol (RTP) to stream the requested content to the multimedia streaming application launched on the mobile device 100. In this embodiment, the application server 106 is part of a core network 108, which is an IP Multimedia Services (IMS) network responsible for session control and Quality of Service (QoS) management of ongoing application sessions. Alternately, the application server 106 is located outside of the core network 108, whereby the core network 108 connects to the application server 106 via the Internet 110. In embodiments where the IMS core network 108 is not implemented, the application server 106 may be part of one of the access networks 102, 104, for example, or it may connect to the access networks 102, 104 via the Internet 110. **[0014]** As illustrated in FIG. 1, the access networks 102, 104 interface with the mobile device 100 in accordance with a network interface specification 112. Preferably, the network interface specification 112 complies with one or more wireless access standards, each having corresponding data handling capabilities, such as average and maximum uplink/downlink throughput speeds. In embodiments, the wireless network standards include CDMA 2000 1X, 1xEV-DO, 1xEV-DV, EDGE, and HSPDA network technologies, or combinations thereof In order to launch the application 106, the mobile device 100 typically accesses its home network 102. However, when the access network 102 is not available, such as when the mobile device 100

	travels outside of its home coverage area, the mobile device 100 is capable of launching the application 106 via a roaming network 104. **[0015]** Turning to FIG. 2, embodiments of the mobile device 200 and networks 214, 220 are provided in accordance with an embodiment of the present invention, wherein the mobile device 200 controls access to one or more applications 202-206 based on access conditions associated with the access networks 214, 220. The mobile device 200 is capable of launching one or more applications 202-206 from its memory. The applications 202-206 include multimedia, voice, email, instant messaging, text messaging, firmware update, or any other applications or services requiring access to the home network 214 or roaming network 220 to establish an application session. In the illustrated embodiment, the memory of the mobile device 200 includes a Firmware Update Over the Air (FOTA) application 202, a Voice over IP (VoIP) application 204, and a video streaming application 206. **[0016]** To prevent one or more applications or services 202-206 from running when the access conditions are not suitable, the memory of the mobile device 200 includes a policy or application access database 212, which is used to store a list of access conditions that are inappropriate for launching the applications 202-206. Specifically, the access conditions are based on the type of the current access network used by the mobile device 200 for launching or maintaining the requested application session 202-206. For example, the access conditions may indicate whether the mobile device is currently accessing its home network 214 or roaming on the network 220. Similarly, the access conditions may indicate the type of network access interface or standard used by the current network 214, 220 to provide data connection necessary to run the application 202-206. The following table illustrates an example of the policy database 212 having a list of applications and corresponding access conditions, which in this embodiment are designated as inappropriate for allowing access to the listed applications or services. **[0017]** Alternatively, the database 212 may contain a list of application/access condition pairs under which access to the requested applications or services is allowed. In embodiments, the policy database 212 includes application types, such as “video streaming” and/or associated application names, such as “Windows Media Player,” for example. As illustrated above, the policy database 212 correlates predetermined actions with current status of access conditions associated with a given application session. When the mobile device 200 registers with an access network having a network access technology specification 222 with insufficient data handling capabilities for the requested application, the mobile device 200 is instructed to deny access to a data-intensive application or service specified in the database or lookup table 212. For example, the mobile device 200 is instructed to deny access to a video streaming or VoIP application session when the access conditions indicate that the mobile device 200 is currently using a CDMA 2000 1x network access technology. This avoids unnecessary use of network resources which, under current access conditions, are incapable of providing a satisfying user experience for the desired application. On the other hand, if the current access

	conditions do not match those in the policy database 212, such as when the mobile device 200 is registered with an EVDO access network, a user is granted full access to the desired video streaming or VoIP applications. Similarly, to avoid unwanted roaming charges, the policy database 212 includes instructions to suspend any scheduled firmware updates via a FOTA application until the mobile device 200 returns to the home network 214. **[0018]** Preferably, the policy database 212 is populated by a network provider using conventional Over the Air Device Management (OTA DM) technology to provide the network operator with full control over the contents of the database 212. In an embodiment, the policy database 212 is centrally populated, distributed, and updated over the air for each mobile device 200 via a management console 218 connected to a device management server 216. The network provider may choose to distribute the policy database 212 according to different classes of mobile devices 200, wherein each device class designates the types of access networks accessible to the device 200, as well as the types of applications installed in its memory. The management console 218, as well as the device management server 216, are located within the home access network 214 or may be collocated with the network administration equipment at a network operations center (NOC) or at a mobile switching center (MSC), for example. **[0019]** As further illustrated in FIG. 2, to gain access to the network resources, the application 202-206 registers with an application manager 210. Specifically, when a user attempts to launch an application 202-206, the application 202-206 supplies its name and/or type information to the application manager 210, which, in turn, receives an input of the monitored access conditions from the access network monitor 208. The application manager 210 queries the policy database 212 for the corresponding application/access condition entry and denies access to the application if a match is found. Otherwise, the mobile device 200 initiates the application session over the current access network 214, 220. In a further embodiment, the access network monitor 208 continues to report the changes in current access conditions during the application session to allow the application manager 210 to terminate the application when a change in the access conditions matches an entry in the policy database 212. **[0020]** In this embodiment, the application manager 210 and the access network monitor 208 are implemented as Binary Runtime Environment for Wireless (BREW) software modules exposing standard interfaces for interaction with other software components of the mobile device 200 via an application programming interface (API). Other embodiments of the application manager 210 and access network monitor 208 include using a Java-based implementation capable of running on a plurality of mobile phone operating systems, such as Symbian, Windows Mobile Edition, or Palm, for example.

	[0021] Turning to FIG. 3, an embodiment of a method for controlling access to applications from a mobile device 200 is illustrated with reference to an exemplary message flow scenario. In step 300, the device management server 216 updates the policy database 212 when new applications or services are introduced by the network operator or pursuant to setting up a new customer account. In step 302, when the user requests to launch a video streaming application 206, the application 206 registers with the application manager 210 by providing it with its name and/or type information, such as "Windows Media Player"/"video streaming," for example. This prompts the application manager 2 10 to request and receive the current access condition information from the access network monitor 208, steps 304-306. In this embodiment, the access condition information includes information regarding the current access network, such as roaming status and compatible network access technology. In steps 308-310, based on the received application information, the application manager 210 requests and receives one or more entries from the policy database 212 indicating which access conditions preclude the establishment of an application session for the application 206. In step 312, the application manager allows the user to launch the requested application if the current access conditions do not match any of the entries returned by the policy database 212 that require denial or suspension of access to the application. In this embodiment, upon establishment of the application session, the access network monitor 208 continuously monitors any changes in the current access conditions. Therefore, when, in step 314, the access network monitor 208 detects a change in the access conditions, for example when the mobile device 200 migrates from an EVDO to a CDMA 2000 1X access network overlay, it notifies the application manager 210 accordingly. Since this change in the access conditions matches an entry received from the policy database 212 requiring denial of access to the application, the application manager 210, in step 316, sends an event to the application 206 ending the current application session by forcing it to quit. *See* Figs. 1, 2 & 3. To the extent Abichandani does not explicitly and/or inherently disclose this element, it would have been obvious in view of the knowledge of a person of ordinary skill in the art in light of Abichandani alone or it would have been obvious to combine Abichandani with one or more prior art references charted in these Invalidity Contentions or identified in the cover document to which this chart is attached.

ii. classify whether a particular application capable of both interacting with the user in a user interface foreground of the device, and at least some Internet service activities when not interacting with the user in the device user interface foreground, is interacting with the user in the device user interface foreground, and	Abichandani discloses this limitation. For example: **[Abstract]** A system and method are described whereby a mobile device controls access to mobile applications based on access conditions associated with a current access network. To prevent mobile applications from running when the access conditions are not suitable, the mobile device includes a policy database used to store a list of access conditions that are inappropriate for launching the installed applications. The access conditions are based on the type of the current access network used by the mobile device for launching or maintaining the requested application session. The access conditions indicate whether the mobile device is currently accessing its home network or roaming on another provider's network. Similarly, the access conditions indicate the type of network access interface used by the current network to provide the data connection necessary to run the requested application. The policy database correlates predetermined actions with the access conditions associated with a given application session. **[0004]** Embodiments of the invention are used to provide a system and method for controlling access to mobile applications from the mobile device based on access conditions associated with a current access network, To prevent one or more applications or services from running when the access conditions are not suitable, the memory of the mobile device includes a policy or application access database, which is used to store a list of access conditions that are inappropriate for launching the installed applications. In embodiments, the access conditions are based on the type of the current access network used by the mobile device for launching or maintaining the requested application session. For example, the access conditions may indicate whether the mobile device is currently accessing its home network or roaming on another provider's network. Similarly, the access conditions may indicate the type of network access interface used by the current network to provide the data connection necessary to run the requested application. The policy database correlates predetermined actions with current status of access conditions associated with a given application session. In one embodiment, when the mobile device accesses a network having an access technology specification with insufficient data handling capabilities for the requested application, the mobile device denies access to the data-intensive application or service specified in the policy database. Similarly, to avoid unwanted roaming charges, the mobile device's policy database includes instructions to suspend any scheduled firmware updates via a firmware over the air (FOTA) application until the mobile device returns to its home network. **[0005]** In one aspect of the invention, a method is provided for controlling access to an application, the application capable of running on a mobile device by connecting to an access network, the method comprising registering the application with the mobile device, populating a record on the mobile device, the record specifying one or more conditions for controlling access to the application, the one or more conditions associated with the access network, monitoring the one or more conditions, and controlling access to the application from the mobile device based on the one or more conditions.

	[0006] In another aspect of the invention, a mobile device is provided, the mobile device capable of running an application by connecting to an access network, the mobile device comprising a processor, a wireless interface for connecting to the access network, and a computer readable medium having thereon instructions for registering the application with the mobile device, populating a record on the mobile device, the record specifying one or more conditions for controlling access to the application, the one or more conditions associated with the access network, monitoring the one or more conditions, and controlling access to the application from the mobile device based on the one or more conditions. **[0007]** In still another aspect of the invention, a system is provided for controlling access to an application, the application capable of running on a mobile device by connecting to an access network, the system comprising (a) the mobile device capable of storing a record for specifying one or more conditions for controlling access to the application, the one or more conditions associated with the access network, the mobile device comprising an access network monitor module configured to monitor the one or more conditions, and an application manager module configured to control access to the application from the mobile device based on the one or more conditions reported by the access network monitor module, and (b) a device management server having a management connection to the mobile device for populating the record. **[0013]** Turning to FIG. 1, an implementation of a system contemplated by an embodiment of the invention is shown with reference to a mobile network environment. In the illustrated embodiment, the user device 100 is a mobile device, such as a wireless telephone or a portable computer capable of launching an application by connecting to an application server 106 via one or more access networks 102, 104. The application server 106 is responsible for content delivery to the one or more applications running on a mobile device 100. For example, when the mobile device 100 includes a multimedia streaming application, the application server 106 employs a Real-Time Transfer Protocol (RTP) to stream the requested content to the multimedia streaming application launched on the mobile device 100. In this embodiment, the application server 106 is part of a core network 108, which is an IP Multimedia Services (IMS) network responsible for session control and Quality of Service (QoS) management of ongoing application sessions. Alternately, the application server 106 is located outside of the core network 108, whereby the core network 108 connects to the application server 106 via the Internet 110. In embodiments where the IMS core network 108 is not implemented, the application server 106 may be part of one of the access networks 102, 104, for example, or it may connect to the access networks 102, 104 via the Internet 110. **[0014]** As illustrated in FIG. 1, the access networks 102, 104 interface with the mobile device 100 in accordance with a network interface specification 112. Preferably, the network interface specification 112 complies with one or more wireless access standards, each having corresponding data handling capabilities,

	such as average and maximum uplink/downlink throughput speeds. In embodiments, the wireless network standards include CDMA 2000 1X, 1xEV-DO, 1xEV-DV, EDGE, and HSPDA network technologies, or combinations thereof In order to launch the application 106, the mobile device 100 typically accesses its home network 102. However, when the access network 102 is not available, such as when the mobile device 100 travels outside of its home coverage area, the mobile device 100 is capable of launching the application 106 via a roaming network 104. **[0015]** Turning to FIG. 2, embodiments of the mobile device 200 and networks 214, 220 are provided in accordance with an embodiment of the present invention, wherein the mobile device 200 controls access to one or more applications 202-206 based on access conditions associated with the access networks 214, 220. The mobile device 200 is capable of launching one or more applications 202-206 from its memory. The applications 202-206 include multimedia, voice, email, instant messaging, text messaging, firmware update, or any other applications or services requiring access to the home network 214 or roaming network 220 to establish an application session. In the illustrated embodiment, the memory of the mobile device 200 includes a Firmware Update Over the Air (FOTA) application 202, a Voice over IP (VoIP) application 204, and a video streaming application 206. **[0016]** To prevent one or more applications or services 202-206 from running when the access conditions are not suitable, the memory of the mobile device 200 includes a policy or application access database 212, which is used to store a list of access conditions that are inappropriate for launching the applications 202-206. Specifically, the access conditions are based on the type of the current access network used by the mobile device 200 for launching or maintaining the requested application session 202-206. For example, the access conditions may indicate whether the mobile device is currently accessing its home network 214 or roaming on the network 220. Similarly, the access conditions may indicate the type of network access interface or standard used by the current network 214, 220 to provide data connection necessary to run the application 202-206. The following table illustrates an example of the policy database 212 having a list of applications and corresponding access conditions, which in this embodiment are designated as inappropriate for allowing access to the listed applications or services. **[0017]** Alternatively, the database 212 may contain a list of application/access condition pairs under which access to the requested applications or services is allowed. In embodiments, the policy database 212 includes application types, such as “video streaming” and/or associated application names, such as “Windows Media Player,” for example. As illustrated above, the policy database 212 correlates predetermined actions with current status of access conditions associated with a given application session. When the mobile device 200 registers with an access network having a network access technology specification 222 with insufficient data handling capabilities for the requested application, the mobile device 200 is instructed to deny access to a data-intensive application or service specified in the database or lookup table 212. For example, the mobile

	device 200 is instructed to deny access to a video streaming or VoIP application session when the access conditions indicate that the mobile device 200 is currently using a CDMA 2000 1x network access technology. This avoids unnecessary use of network resources which, under current access conditions, are incapable of providing a satisfying user experience for the desired application. On the other hand, if the current access conditions do not match those in the policy database 212, such as when the mobile device 200 is registered with an EVDO access network, a user is granted full access to the desired video streaming or VoIP applications. Similarly, to avoid unwanted roaming charges, the policy database 212 includes instructions to suspend any scheduled firmware updates via a FOTA application until the mobile device 200 returns to the home network 214. **[0018]** Preferably, the policy database 212 is populated by a network provider using conventional Over the Air Device Management (OTA DM) technology to provide the network operator with full control over the contents of the database 212. In an embodiment, the policy database 212 is centrally populated, distributed, and updated over the air for each mobile device 200 via a management console 218 connected to a device management server 216. The network provider may choose to distribute the policy database 212 according to different classes of mobile devices 200, wherein each device class designates the types of access networks accessible to the device 200, as well as the types of applications installed in its memory. The management console 218, as well as the device management server 216, are located within the home access network 214 or may be collocated with the network administration equipment at a network operations center (NOC) or at a mobile switching center (MSC), for example. **[0019]** As further illustrated in FIG. 2, to gain access to the network resources, the application 202-206 registers with an application manager 210. Specifically, when a user attempts to launch an application 202-206, the application 202-206 supplies its name and/or type information to the application manager 210, which, in turn, receives an input of the monitored access conditions from the access network monitor 208. The application manager 210 queries the policy database 212 for the corresponding application/access condition entry and denies access to the application if a match is found. Otherwise, the mobile device 200 initiates the application session over the current access network 214, 220. In a further embodiment, the access network monitor 208 continues to report the changes in current access conditions during the application session to allow the application manager 210 to terminate the application when a change in the access conditions matches an entry in the policy database 212. **[0020]** In this embodiment, the application manager 210 and the access network monitor 208 are implemented as Binary Runtime Environment for Wireless (BREW) software modules exposing standard interfaces for interaction with other software components of the mobile device 200 via an application programming interface (API). Other embodiments of the application manager 210 and access network monitor 208 include using a

	Java-based implementation capable of running on a plurality of mobile phone operating systems, such as Symbian, Windows Mobile Edition, or Palm, for example. **[0021]** Turning to FIG. 3, an embodiment of a method for controlling access to applications from a mobile device 200 is illustrated with reference to an exemplary message flow scenario. In step 300, the device management server 216 updates the policy database 212 when new applications or services are introduced by the network operator or pursuant to setting up a new customer account. In step 302, when the user requests to launch a video streaming application 206, the application 206 registers with the application manager 210 by providing it with its name and/or type information, such as "Windows Media Player"/"video streaming," for example. This prompts the application manager 2 10 to request and receive the current access condition information from the access network monitor 208, steps 304-306. In this embodiment, the access condition information includes information regarding the current access network, such as roaming status and compatible network access technology. In steps 308-310, based on the received application information, the application manager 210 requests and receives one or more entries from the policy database 212 indicating which access conditions preclude the establishment of an application session for the application 206. In step 312, the application manager allows the user to launch the requested application if the current access conditions do not match any of the entries returned by the policy database 212 that require denial or suspension of access to the application. In this embodiment, upon establishment of the application session, the access network monitor 208 continuously monitors any changes in the current access conditions. Therefore, when, in step 314, the access network monitor 208 detects a change in the access conditions, for example when the mobile device 200 migrates from an EVDO to a CDMA 2000 1X access network overlay, it notifies the application manager 210 accordingly. Since this change in the access conditions matches an entry received from the policy database 212 requiring denial of access to the application, the application manager 210, in step 316, sends an event to the application 206 ending the current application session by forcing it to quit. *See* Figs. 1, 2 & 3. To the extent Abichandani does not explicitly and/or inherently disclose this element, it would have been obvious in view of the knowledge of a person of ordinary skill in the art in light of Abichandani alone or it would have been obvious to combine Abichandani with one or more prior art references charted in these Invalidity Contentions or identified in the cover document to which this chart is attached.
(f) selectively allow or deny one or more Internet service activities by or on behalf of the particular application based on whether or not the particular application is one of the first one or more applications,	Abichandani discloses this limitation. For example: **[Abstract]** A system and method are described whereby a mobile device controls access to mobile applications based on access conditions associated with a current access network. To prevent mobile applications from running when the access conditions are not suitable, the mobile device includes a policy

the differential traffic control policy, including any applicable user augmentation of the differential traffic control policy, and the classifications performed by the one or more processors.	database used to store a list of access conditions that are inappropriate for launching the installed applications. The access conditions are based on the type of the current access network used by the mobile device for launching or maintaining the requested application session. The access conditions indicate whether the mobile device is currently accessing its home network or roaming on another provider's network. Similarly, the access conditions indicate the type of network access interface used by the current network to provide the data connection necessary to run the requested application. The policy database correlates predetermined actions with the access conditions associated with a given application session. **[0004]** Embodiments of the invention are used to provide a system and method for controlling access to mobile applications from the mobile device based on access conditions associated with a current access network, To prevent one or more applications or services from running when the access conditions are not suitable, the memory of the mobile device includes a policy or application access database, which is used to store a list of access conditions that are inappropriate for launching the installed applications. In embodiments, the access conditions are based on the type of the current access network used by the mobile device for launching or maintaining the requested application session. For example, the access conditions may indicate whether the mobile device is currently accessing its home network or roaming on another provider's network. Similarly, the access conditions may indicate the type of network access interface used by the current network to provide the data connection necessary to run the requested application. The policy database correlates predetermined actions with current status of access conditions associated with a given application session. In one embodiment, when the mobile device accesses a network having an access technology specification with insufficient data handling capabilities for the requested application, the mobile device denies access to the data-intensive application or service specified in the policy database. Similarly, to avoid unwanted roaming charges, the mobile device's policy database includes instructions to suspend any scheduled firmware updates via a firmware over the air (FOTA) application until the mobile device returns to its home network. **[0005]** In one aspect of the invention, a method is provided for controlling access to an application, the application capable of running on a mobile device by connecting to an access network, the method comprising registering the application with the mobile device, populating a record on the mobile device, the record specifying one or more conditions for controlling access to the application, the one or more conditions associated with the access network, monitoring the one or more conditions, and controlling access to the application from the mobile device based on the one or more conditions. **[0006]** In another aspect of the invention, a mobile device is provided, the mobile device capable of running an application by connecting to an access network, the mobile device comprising a processor, a wireless interface for connecting to the access network, and a computer readable medium having thereon instructions for registering the application with the mobile device, populating a record on the mobile device, the record

	specifying one or more conditions for controlling access to the application, the one or more conditions associated with the access network, monitoring the one or more conditions, and controlling access to the application from the mobile device based on the one or more conditions. **[0007]** In still another aspect of the invention, a system is provided for controlling access to an application, the application capable of running on a mobile device by connecting to an access network, the system comprising (a) the mobile device capable of storing a record for specifying one or more conditions for controlling access to the application, the one or more conditions associated with the access network, the mobile device comprising an access network monitor module configured to monitor the one or more conditions, and an application manager module configured to control access to the application from the mobile device based on the one or more conditions reported by the access network monitor module, and (b) a device management server having a management connection to the mobile device for populating the record. **[0013]** Turning to FIG. 1, an implementation of a system contemplated by an embodiment of the invention is shown with reference to a mobile network environment. In the illustrated embodiment, the user device 100 is a mobile device, such as a wireless telephone or a portable computer capable of launching an application by connecting to an application server 106 via one or more access networks 102, 104. The application server 106 is responsible for content delivery to the one or more applications running on a mobile device 100. For example, when the mobile device 100 includes a multimedia streaming application, the application server 106 employs a Real-Time Transfer Protocol (RTP) to stream the requested content to the multimedia streaming application launched on the mobile device 100. In this embodiment, the application server 106 is part of a core network 108, which is an IP Multimedia Services (IMS) network responsible for session control and Quality of Service (QoS) management of ongoing application sessions. Alternately, the application server 106 is located outside of the core network 108, whereby the core network 108 connects to the application server 106 via the Internet 110. In embodiments where the IMS core network 108 is not implemented, the application server 106 may be part of one of the access networks 102, 104, for example, or it may connect to the access networks 102, 104 via the Internet 110. **[0014]** As illustrated in FIG. 1, the access networks 102, 104 interface with the mobile device 100 in accordance with a network interface specification 112. Preferably, the network interface specification 112 complies with one or more wireless access standards, each having corresponding data handling capabilities, such as average and maximum uplink/downlink throughput speeds. In embodiments, the wireless network standards include CDMA 2000 1X, 1xEV-DO, 1xEV-DV, EDGE, and HSPDA network technologies, or combinations thereof In order to launch the application 106, the mobile device 100 typically accesses its home network 102. However, when the access network 102 is not available, such as when the mobile device 100

	travels outside of its home coverage area, the mobile device 100 is capable of launching the application 106 via a roaming network 104. **[0015]** Turning to FIG. 2, embodiments of the mobile device 200 and networks 214, 220 are provided in accordance with an embodiment of the present invention, wherein the mobile device 200 controls access to one or more applications 202-206 based on access conditions associated with the access networks 214, 220. The mobile device 200 is capable of launching one or more applications 202-206 from its memory. The applications 202-206 include multimedia, voice, email, instant messaging, text messaging, firmware update, or any other applications or services requiring access to the home network 214 or roaming network 220 to establish an application session. In the illustrated embodiment, the memory of the mobile device 200 includes a Firmware Update Over the Air (FOTA) application 202, a Voice over IP (VoIP) application 204, and a video streaming application 206. **[0016]** To prevent one or more applications or services 202-206 from running when the access conditions are not suitable, the memory of the mobile device 200 includes a policy or application access database 212, which is used to store a list of access conditions that are inappropriate for launching the applications 202-206. Specifically, the access conditions are based on the type of the current access network used by the mobile device 200 for launching or maintaining the requested application session 202-206. For example, the access conditions may indicate whether the mobile device is currently accessing its home network 214 or roaming on the network 220. Similarly, the access conditions may indicate the type of network access interface or standard used by the current network 214, 220 to provide data connection necessary to run the application 202-206. The following table illustrates an example of the policy database 212 having a list of applications and corresponding access conditions, which in this embodiment are designated as inappropriate for allowing access to the listed applications or services. **[0017]** Alternatively, the database 212 may contain a list of application/access condition pairs under which access to the requested applications or services is allowed. In embodiments, the policy database 212 includes application types, such as “video streaming” and/or associated application names, such as “Windows Media Player,” for example. As illustrated above, the policy database 212 correlates predetermined actions with current status of access conditions associated with a given application session. When the mobile device 200 registers with an access network having a network access technology specification 222 with insufficient data handling capabilities for the requested application, the mobile device 200 is instructed to deny access to a data-intensive application or service specified in the database or lookup table 212. For example, the mobile device 200 is instructed to deny access to a video streaming or VoIP application session when the access conditions indicate that the mobile device 200 is currently using a CDMA 2000 1x network access technology. This avoids unnecessary use of network resources which, under current access conditions, are incapable of providing a satisfying user experience for the desired application. On the other hand, if the current access

	conditions do not match those in the policy database 212, such as when the mobile device 200 is registered with an EVDO access network, a user is granted full access to the desired video streaming or VoIP applications. Similarly, to avoid unwanted roaming charges, the policy database 212 includes instructions to suspend any scheduled firmware updates via a FOTA application until the mobile device 200 returns to the home network 214. **[0018]** Preferably, the policy database 212 is populated by a network provider using conventional Over the Air Device Management (OTA DM) technology to provide the network operator with full control over the contents of the database 212. In an embodiment, the policy database 212 is centrally populated, distributed, and updated over the air for each mobile device 200 via a management console 218 connected to a device management server 216. The network provider may choose to distribute the policy database 212 according to different classes of mobile devices 200, wherein each device class designates the types of access networks accessible to the device 200, as well as the types of applications installed in its memory. The management console 218, as well as the device management server 216, are located within the home access network 214 or may be collocated with the network administration equipment at a network operations center (NOC) or at a mobile switching center (MSC), for example. **[0019]** As further illustrated in FIG. 2, to gain access to the network resources, the application 202-206 registers with an application manager 210. Specifically, when a user attempts to launch an application 202-206, the application 202-206 supplies its name and/or type information to the application manager 210, which, in turn, receives an input of the monitored access conditions from the access network monitor 208. The application manager 210 queries the policy database 212 for the corresponding application/access condition entry and denies access to the application if a match is found. Otherwise, the mobile device 200 initiates the application session over the current access network 214, 220. In a further embodiment, the access network monitor 208 continues to report the changes in current access conditions during the application session to allow the application manager 210 to terminate the application when a change in the access conditions matches an entry in the policy database 212. **[0020]** In this embodiment, the application manager 210 and the access network monitor 208 are implemented as Binary Runtime Environment for Wireless (BREW) software modules exposing standard interfaces for interaction with other software components of the mobile device 200 via an application programming interface (API). Other embodiments of the application manager 210 and access network monitor 208 include using a Java-based implementation capable of running on a plurality of mobile phone operating systems, such as Symbian, Windows Mobile Edition, or Palm, for example.

	[0021] Turning to FIG. 3, an embodiment of a method for controlling access to applications from a mobile device 200 is illustrated with reference to an exemplary message flow scenario. In step 300, the device management server 216 updates the policy database 212 when new applications or services are introduced by the network operator or pursuant to setting up a new customer account. In step 302, when the user requests to launch a video streaming application 206, the application 206 registers with the application manager 210 by providing it with its name and/or type information, such as "Windows Media Player"/"video streaming," for example. This prompts the application manager 2 10 to request and receive the current access condition information from the access network monitor 208, steps 304-306. In this embodiment, the access condition information includes information regarding the current access network, such as roaming status and compatible network access technology. In steps 308-310, based on the received application information, the application manager 210 requests and receives one or more entries from the policy database 212 indicating which access conditions preclude the establishment of an application session for the application 206. In step 312, the application manager allows the user to launch the requested application if the current access conditions do not match any of the entries returned by the policy database 212 that require denial or suspension of access to the application. In this embodiment, upon establishment of the application session, the access network monitor 208 continuously monitors any changes in the current access conditions. Therefore, when, in step 314, the access network monitor 208 detects a change in the access conditions, for example when the mobile device 200 migrates from an EVDO to a CDMA 2000 1X access network overlay, it notifies the application manager 210 accordingly. Since this change in the access conditions matches an entry received from the policy database 212 requiring denial of access to the application, the application manager 210, in step 316, sends an event to the application 206 ending the current application session by forcing it to quit. *See* Figs. 1, 2 & 3. To the extent Abichandani does not explicitly and/or inherently disclose this element, it would have been obvious in view of the knowledge of a person of ordinary skill in the art in light of Abichandani alone or it would have been obvious to combine Abichandani with one or more prior art references charted in these Invalidity Contentions or identified in the cover document to which this chart is attached.
2. The wireless end-user device of claim 1, wherein based on the differential traffic control policy the one or more processors selectively deny one or more Internet service activities by or on behalf of the particular application when the particular application is one of the first one or more applications, the classified wireless	Abichandani anticipates and/or renders obvious claim 1. *See supra* claim 1. In addition, Abichandani discloses this claim. *See supra* claim 1. To the extent Abichandani does not explicitly and/or inherently disclose this element, it would have been obvious in view of the knowledge of a person of ordinary skill in the art in light of Abichandani alone or it would have been obvious to combine Abichandani with one or more prior art references charted in these Invalidity Contentions or identified in the cover document to which this chart is attached.

network is a WWAN type, and the particular application is classified as not interacting with the user in the device user interface foreground.	
3. The wireless end-user device of claim 2, wherein the one or more processors are further configured to override the selective denial of one or more Internet service activities by or on behalf of the particular application when the user has augmented the differential traffic control policy so as to indicate that Internet service activities are allowable when the classified wireless network is the WWAN type, and the particular application is classified as not interacting with the user in the device user interface foreground.	Abichandani anticipates and/or renders obvious claim 2. *See supra* claims 1, 2. In addition, Abichandani discloses this claim. *See supra* claims 1, 2. To the extent Abichandani does not explicitly and/or inherently disclose this element, it would have been obvious in view of the knowledge of a person of ordinary skill in the art in light of Abichandani alone or it would have been obvious to combine Abichandani with one or more prior art references charted in these Invalidity Contentions or identified in the cover document to which this chart is attached.
4. The wireless end-user device of claim 2, wherein based on the differential traffic control policy the one or more processors selectively allow one or more Internet service activities by or on behalf of the particular application when the particular application is one of the first one or more applications, the classified wireless network is the WWAN type, and the particular application is classified as interacting with the user in the device user interface foreground.	Abichandani anticipates and/or renders obvious claim 2. *See supra* claims 1, 2. In addition, Abichandani discloses this claim. *See supra* claims 1, 2. To the extent Abichandani does not explicitly and/or inherently disclose this element, it would have been obvious in view of the knowledge of a person of ordinary skill in the art in light of Abichandani alone or it would have been obvious to combine Abichandani with one or more prior art references charted in these Invalidity Contentions or identified in the cover document to which this chart is attached.
5. The wireless end-user device of claim 1, wherein based on the differential traffic control policy the one or more processors selectively allow one or more Internet service activities by or on behalf of a second particular application and/or service when the second particular	Abichandani anticipates and/or renders obvious claim 1. *See supra* claim 1. In addition, Abichandani discloses this claim. *See supra* claim 1. To the extent Abichandani does not explicitly and/or inherently disclose this element, it would have been obvious in view of the knowledge of a person of ordinary skill in the art in light of Abichandani alone or it

application and/or service is one of the second one or more applications and/or services and the classified wireless network is the WWAN type.	would have been obvious to combine Abichandani with one or more prior art references charted in these Invalidity Contentions or identified in the cover document to which this chart is attached.
6. The wireless end-user device of claim 1, wherein the one or more processors are configured to classify that the particular application is interacting with the user in the device user interface foreground when the user of the device is directly interacting with that application or perceiving any benefit from that application.	Abichandani anticipates and/or renders obvious claim 1. *See supra* claim 1. In addition, Abichandani discloses this claim. *See supra* claim 1. To the extent Abichandani does not explicitly and/or inherently disclose this element, it would have been obvious in view of the knowledge of a person of ordinary skill in the art in light of Abichandani alone or it would have been obvious to combine Abichandani with one or more prior art references charted in these Invalidity Contentions or identified in the cover document to which this chart is attached.
7. The wireless end-user device of claim 1, wherein the user interface is further to provide the user of the device with information regarding why the differential traffic control policy is applied to the particular application.	Abichandani anticipates and/or renders obvious claim 1. *See supra* claim 1. In addition, Abichandani discloses this claim. *See supra* claim 1. To the extent Abichandani does not explicitly and/or inherently disclose this element, it would have been obvious in view of the knowledge of a person of ordinary skill in the art in light of Abichandani alone or it would have been obvious to combine Abichandani with one or more prior art references charted in these Invalidity Contentions or identified in the cover document to which this chart is attached.
8. The wireless end-user device of claim 1, wherein the differential traffic control policy is part of a multimode profile having different policies for different ones of the network types.	Abichandani anticipates and/or renders obvious claim 1. *See supra* claim 1. In addition, Abichandani discloses this claim. *See supra* claim 1. To the extent Abichandani does not explicitly and/or inherently disclose this element, it would have been obvious in view of the knowledge of a person of ordinary skill in the art in light of Abichandani alone or it would have been obvious to combine Abichandani with one or more prior art references charted in these Invalidity Contentions or identified in the cover document to which this chart is attached.
9. The wireless end-user device of claim 8, wherein the one or more processors are further configured to select a traffic control policy from the multimode profile based at least in part on the classified wireless network type.	Abichandani anticipates and/or renders obvious claim 8. *See supra* claims 1, 8. In addition, Abichandani discloses this claim. *See supra* claims 1, 8. To the extent Abichandani does not explicitly and/or inherently disclose this element, it would have been obvious in view of the knowledge of a person of ordinary skill in the art in light of Abichandani alone or it would have been obvious to combine Abichandani with one or more prior art references charted in these Invalidity Contentions or identified in the cover document to which this chart is attached.

10. The wireless end-user device of claim 9, wherein the one or more processors are further configured to, when the classified wireless network type is at least one type of WLAN, select the traffic control policy from the multimode profile based at least in part on a type of network connection from the WLAN to the Internet.	Abichandani anticipates and/or renders obvious claim 9. *See supra* claims 1, 9. In addition, Abichandani discloses this claim. *See supra* claims 1, 9. To the extent Abichandani does not explicitly and/or inherently disclose this element, it would have been obvious in view of the knowledge of a person of ordinary skill in the art in light of Abichandani alone or it would have been obvious to combine Abichandani with one or more prior art references charted in these Invalidity Contentions or identified in the cover document to which this chart is attached.
11. The wireless end-user device of claim 1, wherein the plurality of network types include three or more of 2G, 3G, 4G, home, roaming, and WiFi.	Abichandani anticipates and/or renders obvious claim 1. *See supra* claim 1. In addition, Abichandani discloses this claim. *See supra* claim 1. To the extent Abichandani does not explicitly and/or inherently disclose this element, it would have been obvious in view of the knowledge of a person of ordinary skill in the art in light of Abichandani alone or it would have been obvious to combine Abichandani with one or more prior art references charted in these Invalidity Contentions or identified in the cover document to which this chart is attached.
12. The wireless end-user device of claim 1, the one or more processors further configured to receive an update to at least a portion of the differential traffic control policy list from a network element.	Abichandani anticipates and/or renders obvious claim 1. *See supra* claim 1. In addition, Abichandani discloses this claim. *See supra* claim 1. To the extent Abichandani does not explicitly and/or inherently disclose this element, it would have been obvious in view of the knowledge of a person of ordinary skill in the art in light of Abichandani alone or it would have been obvious to combine Abichandani with one or more prior art references charted in these Invalidity Contentions or identified in the cover document to which this chart is attached.
13. The wireless end-user device of claim 1, wherein the plurality of network types include a roaming WWAN type and a home WWAN type, and the one or more processors are to apply the differential traffic control policy to one of but not both of the roaming WWAN type and the home WWAN type.	Abichandani anticipates and/or renders obvious claim 1. *See supra* claim 1. In addition, Abichandani discloses this claim. *See supra* claim 1. To the extent Abichandani does not explicitly and/or inherently disclose this element, it would have been obvious in view of the knowledge of a person of ordinary skill in the art in light of Abichandani alone or it would have been obvious to combine Abichandani with one or more prior art references charted in these Invalidity Contentions or identified in the cover document to which this chart is attached.
14. The wireless end-user device of claim 1, wherein the plurality of network types include the WWAN type and a WLAN type, and the one or more processors are	Abichandani anticipates and/or renders obvious claim 1. *See supra* claim 1. In addition, Abichandani discloses this claim. *See supra* claim 1.

to apply the differential traffic control policy to one of but not both of the WWAN type and the WLAN type.	To the extent Abichandani does not explicitly and/or inherently disclose this element, it would have been obvious in view of the knowledge of a person of ordinary skill in the art in light of Abichandani alone or it would have been obvious to combine Abichandani with one or more prior art references charted in these Invalidity Contentions or identified in the cover document to which this chart is attached.
15. The wireless end-user device of claim 1, wherein the one or more processors are further configured to dynamically change the application of the differential traffic control policy based on a power state of the device.	Abichandani anticipates and/or renders obvious claim 1. *See supra* claim 1. In addition, Abichandani discloses this claim. *See supra* claim 1. To the extent Abichandani does not explicitly and/or inherently disclose this element, it would have been obvious in view of the knowledge of a person of ordinary skill in the art in light of Abichandani alone or it would have been obvious to combine Abichandani with one or more prior art references charted in these Invalidity Contentions or identified in the cover document to which this chart is attached.
16. The wireless end-user device of claim 1, wherein the one or more processors are further configured to dynamically change the application of the differential traffic control policy based on a device usage state.	Abichandani anticipates and/or renders obvious claim 1. *See supra* claim 1. In addition, Abichandani discloses this claim. *See supra* claim 1. To the extent Abichandani does not explicitly and/or inherently disclose this element, it would have been obvious in view of the knowledge of a person of ordinary skill in the art in light of Abichandani alone or it would have been obvious to combine Abichandani with one or more prior art references charted in these Invalidity Contentions or identified in the cover document to which this chart is attached.
17. The wireless end-user device of claim 1, wherein the one or more processors are further configured to dynamically change the application of the differential traffic control policy based on power control state changes for one or more of the modems.	Abichandani anticipates and/or renders obvious claim 1. *See supra* claim 1. In addition, Abichandani discloses this claim. *See supra* claim 1. To the extent Abichandani does not explicitly and/or inherently disclose this element, it would have been obvious in view of the knowledge of a person of ordinary skill in the art in light of Abichandani alone or it would have been obvious to combine Abichandani with one or more prior art references charted in these Invalidity Contentions or identified in the cover document to which this chart is attached.
18. The wireless end-user device of claim 1, wherein the differential traffic control policy defines that the first one or more applications can only access a first one of the network types during particular time windows.	Abichandani anticipates and/or renders obvious claim 1. *See supra* claim 1. In addition, Abichandani discloses this claim. *See supra* claim 1. To the extent Abichandani does not explicitly and/or inherently disclose this element, it would have been obvious in view of the knowledge of a person of ordinary skill in the art in light of Abichandani alone or it would have been obvious to combine Abichandani with one or more prior art references charted in these Invalidity Contentions or identified in the cover document to which this chart is attached.

19. The wireless end-user device of claim 1, wherein the one or more processors are configured to classify that the particular application is interacting with the user in the device user interface foreground based on a state of user interface priority for the application.	Abichandani anticipates and/or renders obvious claim 1. *See supra* claim 1. In addition, Abichandani discloses this claim. *See supra* claim 1. To the extent Abichandani does not explicitly and/or inherently disclose this element, it would have been obvious in view of the knowledge of a person of ordinary skill in the art in light of Abichandani alone or it would have been obvious to combine Abichandani with one or more prior art references charted in these Invalidity Contentions or identified in the cover document to which this chart is attached.
20. The wireless end-user device of claim 1, wherein the second one or more applications are not subject to a differential network access control that is applicable to the first one or more applications.	Abichandani anticipates and/or renders obvious claim 1. *See supra* claim 1. In addition, Abichandani discloses this claim. *See supra* claim 1. To the extent Abichandani does not explicitly and/or inherently disclose this element, it would have been obvious in view of the knowledge of a person of ordinary skill in the art in light of Abichandani alone or it would have been obvious to combine Abichandani with one or more prior art references charted in these Invalidity Contentions or identified in the cover document to which this chart is attached.
21. The wireless end-user device of claim 1, wherein the one or more processors are further configured to classify between: user applications; system applications, utilities, functions, or processes; and operating system application, utilities, functions, or processes.	Abichandani anticipates and/or renders obvious claim 1. *See supra* claim 1. In addition, Abichandani discloses this claim. *See supra* claim 1. To the extent Abichandani does not explicitly and/or inherently disclose this element, it would have been obvious in view of the knowledge of a person of ordinary skill in the art in light of Abichandani alone or it would have been obvious to combine Abichandani with one or more prior art references charted in these Invalidity Contentions or identified in the cover document to which this chart is attached.
22. The wireless end-user device of claim 1, wherein the second one or more applications or services comprises foreground services.	Abichandani anticipates and/or renders obvious claim 1. *See supra* claim 1. In addition, Abichandani discloses this claim. *See supra* claim 1. To the extent Abichandani does not explicitly and/or inherently disclose this element, it would have been obvious in view of the knowledge of a person of ordinary skill in the art in light of Abichandani alone or it would have been obvious to combine Abichandani with one or more prior art references charted in these Invalidity Contentions or identified in the cover document to which this chart is attached.
23. The wireless end-user device of claim 1, wherein selectively deny comprises intermittently block when the one or more Internet service activities are requested during selected time windows.	Abichandani anticipates and/or renders obvious claim 1. *See supra* claim 1. In addition, Abichandani discloses this claim. *See supra* claim 1.

	To the extent Abichandani does not explicitly and/or inherently disclose this element, it would have been obvious in view of the knowledge of a person of ordinary skill in the art in light of Abichandani alone or it would have been obvious to combine Abichandani with one or more prior art references charted in these Invalidity Contentions or identified in the cover document to which this chart is attached.
24. The wireless end-user device of claim 1, wherein the one or more processors are configured to prevent the first one or more applications from changing the power state of at least one of the modems, and to not prevent the second one or more applications from changing the power state of the same modem or modems.	Abichandani anticipates and/or renders obvious claim 1. *See supra* claim 1. In addition, Abichandani discloses this claim. *See supra* claim 1. To the extent Abichandani does not explicitly and/or inherently disclose this element, it would have been obvious in view of the knowledge of a person of ordinary skill in the art in light of Abichandani alone or it would have been obvious to combine Abichandani with one or more prior art references charted in these Invalidity Contentions or identified in the cover document to which this chart is attached.